



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000041102 A**(43) Date of publication of application: **08.02.00**

(51) Int. Cl.

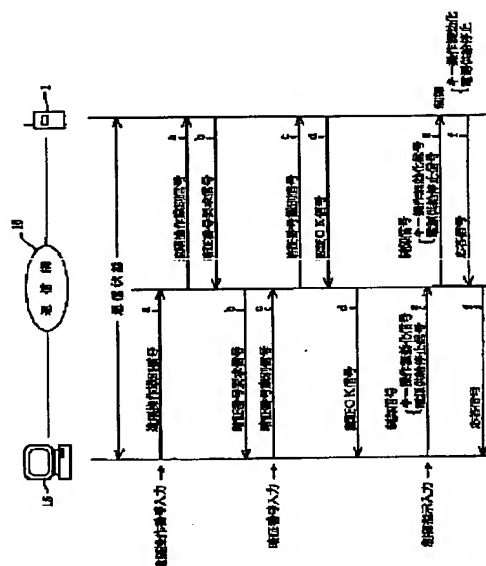
H04M 1/66**H04Q 7/38****H04M 1/00****H04M 11/00**(21) Application number: **10205340**(71) Applicant: **DENSO CORP**(22) Date of filing: **21.07.98**(72) Inventor: **KONDO HIROMASA**(54) **RADIO COMMUNICATION DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To obtain a radio communication device that can be controlled remotely.

SOLUTION: When a user operates a personal computer 15 and a portable telephone set 1 receives a control signal (refer to e in figure) transmitted from the personal computer 15, a control circuit of the portable telephone set 1 conducts control in response to the control signal e.g. the invalidation of key operation or the stop of power supply in the portable telephone set 1. If the personal computer 15 is present even in the case that the portable telephone set 1 is not present at home, the user operates the personal computer 15 to be able to control remotely the portable telephone set such as the invalidation of the key operations of the portable telephone set 1 or the stop of the power supply to the portable telephone set 1.

COPYRIGHT: (C)2000,JPO



portable telephone device 1 is inputted, for example "#", "0", "0", "0", "0" which is allocated as a remote control number, the PC 15 is caused to transmit a remote control recognition signal (see a in Fig. 1) in which the remote control number thereof is stored. When the remote control recognition signal transmitted from the PC 15 is received in the portable telephone device 1 via the communication network 16, the control circuit 8 of the portable telephone device 1 advances to remote control processing and transmits an identification number request signal (see b in Fig. 1). The control circuit 8 of the portable telephone device 1 then awaits reception of an identification number.

[0023]

When the identification number request signal transmitted from the portable telephone device 1 is received in the PC 15 via the communication network 16, the PC 15 displays an identification number input screen on a display. In so doing,

In Fig. 1, a personal computer (to be abbreviated to PC hereinafter) 15 has a communication function constituted by a modem, terminal adapter, or the like, and hence serves as the device having a wireless communication function of the present invention. The PC 15 and portable telephone device 1 are constituted so as to be capable of communication via a communication network 16. Note that here, the communication network 16 is a general item including not only a telephone communication network constituted by an ISDN public line, analog public line, or similar, but also an electronic mail communication network incorporating the Internet. Further, it is assumed that the portable telephone device 1 is switched on.

[0022]

First, when the PC 15 and portable telephone device 1 are in a state of communication, the user operates the PC 15, and when a predetermined operation for remote-controlling the

the user is able to perform the next operation, i.e. inputting an identification number.

[0024]

Next, when the user inputs numerals allocated as an identification number, the PC 15 is caused to transmit an identification number recognition signal (see c in Fig. 1) in which the identification number is stored. When the identification number recognition signal transmitted from the PC 15 is received in the portable telephone device 1 via the communication network 16, the control circuit 8 of the portable telephone device 1 identifies the received identification number, and if the result of the identification is favorable (positive), an authentication OK signal (see d in Fig. 1) is transmitted. The control circuit 8 of the portable telephone device 1 then awaits reception of a control signal.

[0025]

When the authentication OK signal transmitted from the

portable telephone device 1 is received in the PC 15 via the communication network 16, the PC 15 displays a control instruction input screen on the display. In so doing, the user is able to perform the next operation, i.e. inputting a control instruction.

[0026]

Here, "control instruction" specifically indicates an instruction to disable key operations, an instruction to cut power supply, an instruction to read voice information, an instruction to read memory dial information, and an instruction to read electronic mail information, and the user may select at will from among these instructions.

[0027]

First, a case in which the user selects an instruction to disable key operations as the control instruction will be described. When the user inputs the instruction to disable key operations as the control instruction, the PC 15 is caused to

transmit a key operation disabling signal as a control signal (see e in Fig. 1). When the key operation disabling signal transmitted from the PC 15 is received in the portable telephone device 1 via the communication network 16, the control circuit 8 of the portable telephone device 1 implements control in accordance with the control signal, in this case disabling subsequent processing relating to key operations in the portable telephone device 1, and then transmits a response signal (see f in Fig. 1).


[0028]

When the response signal transmitted from the portable telephone device 1 is received in the PC 15 via the communication network 16, the PC 15 displays the content of the response, in this case the fact that subsequent processing relating to key operations in the portable telephone device 1 has been disabled, on the display. In so doing, the user is able to recognize this fact.

[0029]

Thus the portable telephone device 1 is constituted such that when a key operation disabling signal is received thereby, subsequent processing relating to key operations is not implemented even when a key operation is performed. In other words, by operating the PC 15 such that the PC 15 transmits a key operation disabling signal, the user is able to disable key operations in the portable telephone device 1. Note that in this case, prohibition of processing relating to key operations is not related to the starting and cutting of the power supply to the portable telephone device 1 which continues to be active.

[0030]

 When the user inputs an instruction to cut power supply as a control instruction, the PC 15 is caused to transmit a power supply cutting signal as a control signal (see e in Fig. 1). When the power supply cutting signal transmitted from the PC 15 is received in the portable telephone device 1 via the

communication network 16, the control circuit 8 of the portable telephone device 1 implements control in accordance with the control signal, in this case cutting the supply of power to the portable telephone device 1, and transmits a response signal (see f in Fig. 1).

[0031]

When the response signal transmitted from the portable telephone device 1 is received in the PC 15 via the communication network 16, the PC 15 displays the content of the response, in this case the fact that power supply to the portable telephone device 1 has been cut, on the display. In so doing, the user is able to recognize this fact.

[0032]

Thus the portable telephone device 1 is constituted such that when a power supply cutting signal is received thereby, subsequent power supply is cut. In other words, by operating the PC 15 such that the PC 15 transmits a power supply cutting

signal, the user can cut the power supply to the portable telephone device 1.

FIG. 1

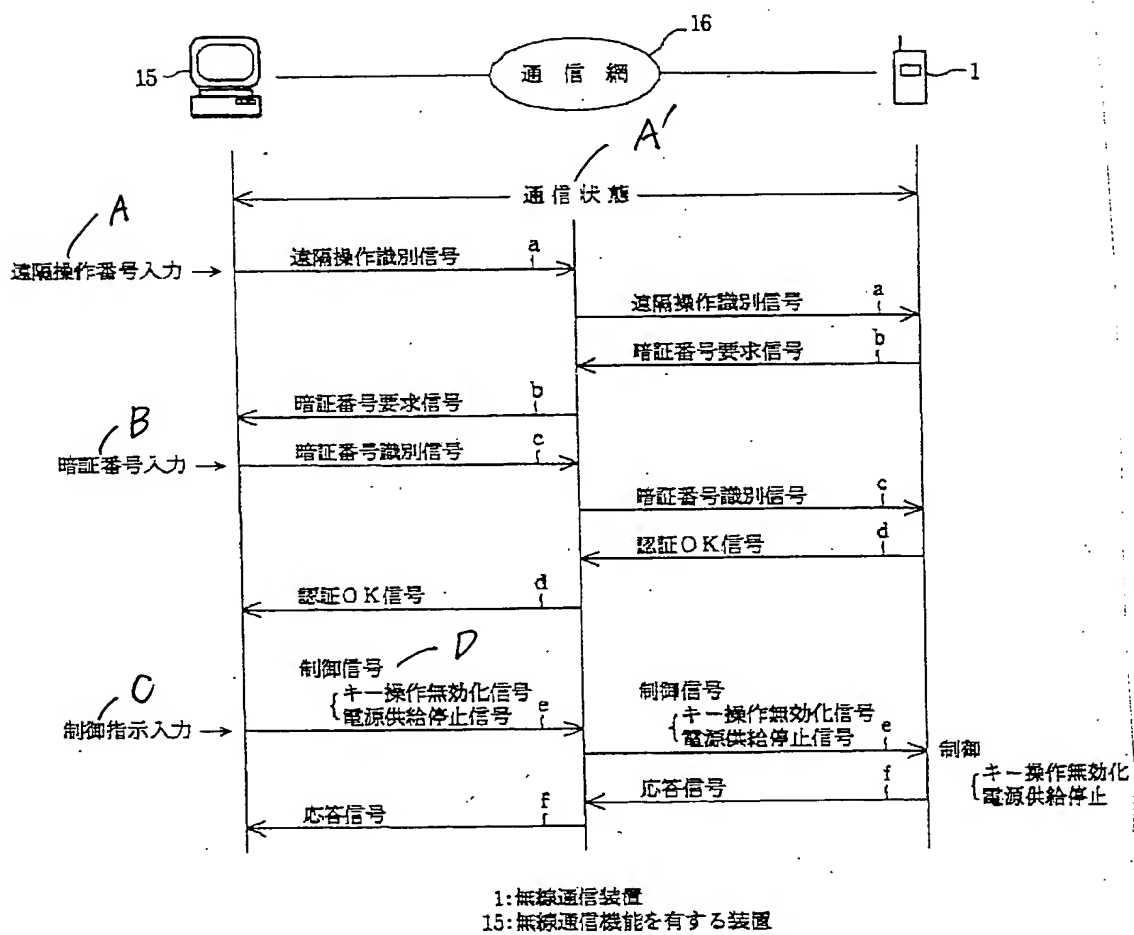


FIG. 1

16 COMMUNICATION NETWORK

A: IN COMMUNICATION

A: INPUT REMOTE CONTROL NUMBER

a REMOTE CONTROL RECOGNITION SIGNAL

a REMOTE CONTROL RECOGNITION SIGNAL

b IDENTIFICATION NUMBER REQUEST SIGNAL

b IDENTIFICATION NUMBER REQUEST SIGNAL

B: INPUT IDENTIFICATION NUMBER

c IDENTIFICATION NUMBER RECOGNITION SIGNAL

c IDENTIFICATION NUMBER RECOGNITION SIGNAL

d AUTHENTICATION OK SIGNAL

d AUTHENTICATION OK SIGNAL

C: INPUT CONTROL INSTRUCTION

e CONTROL SIGNAL {KEY OPERATION DISABLING SIGNAL, POWER
SUPPLY CUTTING SIGNAL

e CONTROL SIGNAL {KEY OPERATION DISABLING SIGNAL, POWER

SUPPLY CUTTING SIGNAL

CONTROL {DISABLE KEY OPERATIONS, CUT POWER SUPPLY

f RESPONSE SIGNAL

f RESPONSE SIGNAL

1 WIRELESS COMMUNICATION DEVICE

15 DEVICE HAVING WIRELESS COMMUNICATION FUNCTION

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-41102

(P2000-41102A)

(43) 公開日 平成12年2月8日 (2000.2.8)

(51) Int.Cl. ⁷	識別記号	F I	テームコード (参考)
H 0 4 M 1/66		H 0 4 M 1/66	A 5 K 0 2 7
H 0 4 Q 7/38		1/00	N 5 K 0 6 7
H 0 4 M 1/00		11/00	3 0 3 5 K 1 0 1
11/00	3 0 3	H 0 4 B 7/26	1 0 9 R

審査請求 未請求 請求項の数10 O L (全 13 頁)

(21) 出願番号 特願平10-205340

(22) 出願日 平成10年7月21日 (1998.7.21)

(71) 出願人 000004260

株式会社デンソー

愛知県刈谷市昭和町1丁目1番地

(72) 発明者 近藤 弘昌

愛知県刈谷市昭和町1丁目1番地 株式会
社デンソー内

(74) 代理人 100071135

弁理士 佐藤 強

Fターム (参考) 5K027 AA11 BB09 BB17 CC08 GG02

HH11 HH24

5K067 AA32 BB04 DD11 DD17 DD27

EED2 HH12 HH22

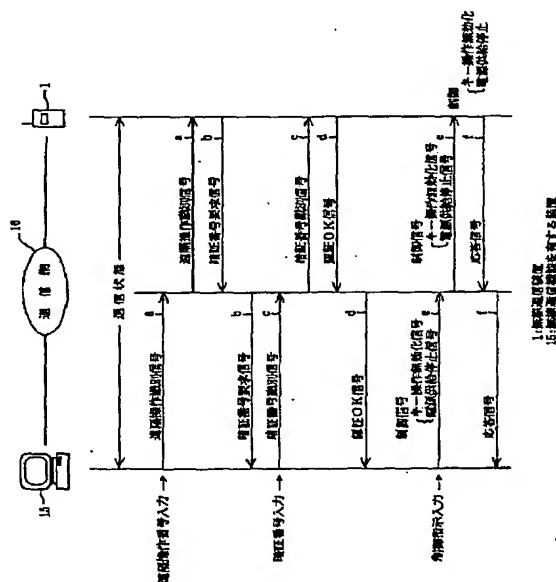
5K101 KK11 LL11 NN45 PP03

(54) 【発明の名称】 無線通信装置

(57) 【要約】

【課題】 遠隔操作されることが可能な無線通信装置を提供する。

【解決手段】 使用者がパソコン15を操作し、パソコン15から送信された制御信号 (図中、e 参照) が携帯電話装置1に受信されると、携帯電話装置1の制御回路は、制御信号に応じた制御、例えば携帯電話装置1におけるキー操作を無効化したり、電源の供給を停止させたりする。使用者は、仮に、携帯電話装置1が手元に存在しない場合でも、パソコン15が存在する環境であれば、そのパソコン15を操作することによって、携帯電話装置1におけるキー操作を無効化したり、電源の供給を停止させたりすることができるなど、携帯電話装置1を遠隔操作することができる。



【特許請求の範囲】

【請求項1】 無線通信機能を有する装置から送信されたキー操作無効化信号を受信可能な受信手段と、この受信手段がキー操作無効化信号を受信したときには、キー操作に対する所定処理の実行を禁止する制御手段とを備えたことを特徴とする無線通信装置。

【請求項2】 キー操作無効化信号を受信したことに応じてキー操作に対する所定処理の実行を禁止するように構成された他の無線通信装置に対して、キー操作無効化信号を送信可能な送信手段と、

キー操作がなされたことを検出可能なキー操作検出手段とを備え、

前記制御手段は、前記キー操作検出手段により所定のキー操作がなされたことを検出したときには、キー操作無効化信号を前記送信手段により送信させるように構成されていることを特徴とする請求項1記載の無線通信装置。

【請求項3】 前記受信手段は、無線通信機能を有する装置もしくは他の無線通信装置から送信された暗証番号を受信可能に構成され、

前記制御手段は、前記受信手段により受信された暗証番号の識別結果が正常であることを条件として、キー操作に対する所定処理の実行の禁止動作を実行するように構成されていることを特徴とする請求項1または2記載の無線通信装置。

【請求項4】 無線通信機能を有する装置から送信された電源供給停止信号を受信可能な受信手段と、この受信手段が電源供給停止信号を受信したときには、電源の供給を停止させる制御手段とを備えたことを特徴とする無線通信装置。

【請求項5】 電源供給停止信号を受信したことに応じて電源の供給が停止されるように構成された他の無線通信装置に対して、電源供給停止信号を送信可能な送信手段と、

キー操作がなされたことを検出可能なキー操作検出手段とを備え、

前記制御手段は、前記キー操作検出手段により所定のキー操作がなされたことを検出したときには、電源供給停止信号を前記送信手段により送信させるように構成されていることを特徴とする請求項4記載の無線通信装置。

【請求項6】 前記受信手段は、無線通信機能を有する装置もしくは他の無線通信装置から送信された暗証番号を受信可能に構成され、

前記制御手段は、前記受信手段により受信された暗証番号の識別結果が正常であることを条件として、電源の供給の停止動作を実行するように構成されていることを特徴とする請求項4または5記載の無線通信装置。

【請求項7】 無線通信機能を有する装置から送信された所定情報読出信号を受信可能な受信手段と、所定情報を格納可能な所定情報格納手段と、

所定情報を送信可能な送信手段と、

前記受信手段が所定情報読出信号を受信したときには、前記所定情報格納手段に格納されている所定情報を前記送信手段により送信させる制御手段とを備えたことを特徴とする無線通信装置。

【請求項8】 キー操作がなされたことを検出可能なキー操作検出手段を備え、

前記送信手段は、所定情報読出信号を受信したことに応じて所定情報格納手段に格納されている所定情報を送信させるように構成された他の無線通信装置に対して、所定情報読出信号を送信可能に構成され、

前記制御手段は、前記キー操作検出手段により所定のキー操作がなされたことを検出したときには、所定情報読出信号を前記送信手段により送信させるように構成されていることを特徴とする請求項7記載の無線通信装置。

【請求項9】 前記受信手段は、無線通信機能を有する装置もしくは他の無線通信装置から送信された暗証番号を受信可能に構成され、

前記制御手段は、前記受信手段により受信された暗証番号の識別結果が正常であることを条件として、所定情報の送信動作を実行するように構成されていることを特徴とする請求項7または8記載の無線通信装置。

【請求項10】 前記所定情報は、音声情報、メモリダイヤル情報もしくは電子メール情報であることを特徴とする請求項7ないし9のいずれかに記載の無線通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯電話装置などの無線通信装置に関する。

【0002】

【発明が解決しようとする課題】近年、無線通信装置としての携帯電話装置が広く普及している。ところで、この携帯電話装置は、携帯できるという点が最大の利点の一つに挙げられるものである。ところが、このことは、換言すれば、使用者が携帯電話装置を携帯している場合には、置き忘れたりする可能性があるということで、場合によっては、紛失してしまう可能性があるということである。そして、仮に、使用者が携帯電話装置を紛失してしまうと、第三者にその携帯電話装置が使用されてしまう虞があるということである。

【0003】このような場合、従来では、例えば、その携帯電話装置を管理している通信事業者に、その旨を連絡すると、通信事業者が交換機のソフトウェアを変更することによって、その携帯電話装置からの発信が禁止され、つまり、第三者がその携帯電話装置を使用することが禁止されるようになるが、この場合には、通信事業者に連絡する手間が必要であったり、迅速性に欠けるという問題があった。

【0004】このように、従来のものは、使用者が自身

の操作によって携帯電話装置を遠隔操作することができない、つまり、携帯電話装置から見れば、遠隔操作されることができないという事情があるため、それに起因して、一例として上述したような問題があり、この点で、利便性に劣るものであった。

【0005】本発明は、上記した事情に鑑みてなされたものであり、その目的は、遠隔操作されることができ、それによって、利便性の向上を図ることができる無線通信装置を提供することにある。

【0006】

【課題を解決するための手段】請求項1記載の無線通信装置によれば、無線通信機能を有する装置からキー操作無効化信号が送信され、そのキー操作無効化信号が受信手段に受信されると、制御手段は、キー操作に対する所定処理の実行を禁止するようになる。したがって、使用者は、仮に、無線通信装置を紛失してしまった場合でも、無線通信機能を有する装置が存在する環境であれば、その無線通信機能を有する装置を操作し、無線通信機能を有する装置からキー操作無効化信号を送信させることによって、無線通信装置におけるキー操作に対する所定処理の実行を禁止することができ、つまり、例えば、第三者が無線通信装置を使用することを禁止することができる。このように、無線通信装置から見れば、遠隔操作されることができ、利便性の向上を図ることができる。尚、この場合、キー操作に対する所定処理の禁止は、無線通信装置における電源の供給開始および供給停止に拘らず、継続して有効となるものである。

【0007】請求項2記載の無線通信装置によれば、キー操作検出手段により所定のキー操作がなされたことが検出されると、制御手段は、キー操作無効化信号を送信手段により送信させるようになる。したがって、使用者は、所定のキー操作を実行することによって、無線通信装置からキー操作無効化信号を送信させ、他の無線通信装置におけるキー操作に対する所定処理の実行を禁止することができ、つまり、上述した無線通信機能を有する装置を操作する代わりに、この無線通信装置を操作することによっても、例えば、第三者が他の無線通信装置を使用することを禁止することができる。このように、無線通信装置から見れば、遠隔操作されるだけでなく、他の無線通信装置を遠隔操作することもできるので、利便性の向上をより図ることができる。

【0008】請求項3記載の無線通信装置によれば、制御手段は、無線通信機能を有する装置もしくは他の無線通信装置から送信された暗証番号の識別結果が正常であることを条件として、キー操作に対する所定処理の実行を禁止するようになる。したがって、使用者は、暗証番号を送信させることによってのみ、キー操作に対する所定処理の実行を禁止することができ、つまり、第三者の操作によって、キー操作に対する所定処理の実行が禁止されることを防止することができ、利便性の向上をより

図ることができる。

【0009】請求項4記載の無線通信装置によれば、無線通信機能を有する装置から電源供給停止信号が送信され、その電源供給停止信号が受信手段に受信されると、制御手段は、電源の供給を停止させるようになる。したがって、使用者は、仮に、無線通信装置を紛失してしまった場合でも、無線通信機能を有する装置が存在する環境であれば、その無線通信機能を有する装置を操作し、無線通信機能を有する装置から電源供給停止信号を送信させることによって、無線通信装置における電源の供給を停止させることができ、つまり、例えば、第三者が無線通信装置を使用することを禁止することができ、また、電力が不要に消費されることも防止することができる。

【0010】請求項5記載の無線通信装置によれば、キー操作検出手段により所定のキー操作がなされたことが検出されると、制御手段は、電源供給停止信号を送信手段により送信させるようになる。したがって、使用者は、所定のキー操作を実行することによって、無線通信装置から電源供給停止信号を送信させ、他の無線通信装置における電源の供給を停止させることができ、つまり、上述した無線通信機能を有する装置を操作する代わりに、この無線通信装置を操作することによっても、例えば、第三者が他の無線通信装置を使用することを禁止することができ、また、電力が不要に消費されることも防止することができる。

【0011】請求項6記載の無線通信装置によれば、制御手段は、無線通信機能を有する装置もしくは他の無線通信装置から送信された暗証番号の識別結果が正常であることを条件として、電源の供給を停止させるようになる。したがって、使用者は、暗証番号を送信させることによってのみ、電源の供給を停止させることができ、つまり、第三者の操作によって、電源の供給が停止されることを防止することができる。

【0012】請求項7記載の無線通信装置によれば、無線通信機能を有する装置から所定情報読出信号が送信され、その所定情報読出信号が受信手段に受信されると、制御手段は、所定情報格納手段に格納されている所定情報を送信手段により送信させるようになる。したがって、使用者は、無線通信機能を有する装置が存在する環境であれば、その無線通信機能を有する装置を操作し、無線通信機能を有する装置から所定情報読出信号を送信させることによって、無線通信装置に格納されている所定情報を読出すことができる。

【0013】請求項8記載の無線通信装置によれば、キー操作検出手段により所定のキー操作がなされたことが検出されると、制御手段は、所定情報読出信号を送信手段により送信させるようになる。したがって、使用者は、所定のキー操作を実行することによって、所定情報読出信号を送信させ、他の無線通信装置に格納されてい

10

20

30

40

50

る所定情報を読出すことができ、つまり、上述した無線通信機能を有する装置を操作する代わりに、この無線通信装置を操作することによっても、他の無線通信装置に格納されている所定情報を読出すことができる。

【0014】請求項9記載の無線通信装置によれば、制御手段は、無線通信機能を有する装置もしくは他の無線通信装置から送信された暗証番号の識別結果が正常であることを条件として、所定情報の送信動作を実行するようになる。したがって、使用者は、暗証番号を送信させることによってのみ、所定情報の送信動作を実行させることができ、つまり、第三者の操作によって、所定情報の送信動作が実行されることを防止することができ、秘密性の向上を図ることができる。

【0015】請求項10記載の無線通信装置によれば、使用者は、無線通信機能を有する装置を操作し、無線通信機能を有する装置から所定情報読出信号を送信させることによって、無線通信装置から所定情報として音声情報、メモリダイヤル情報もしくは電子メール情報を読出すことができる。また、使用者は、所定のキー操作を実行し、無線通信装置から所定情報読出信号を送信させることによって、他の無線通信装置から所定情報として音声情報、メモリダイヤル情報もしくは電子メール情報を読出すことができる。

【0016】

【発明の実施の形態】以下、本発明を携帯電話装置に適用した一実施例について図面を参照して説明する。まず、携帯電話装置の全体構成を示す図2において、携帯電話装置1にあって筐体2の表面側には「開始」キー、「リダイヤル」キー、「終了」キー、「S（スカイウォーカー）」キー、「コール／メモリ」キー、「アップスクロール」キー、「ダウンスクロール」キー、「0」～「9」の数字キー、「＊（アスタリスク）」キー、「＃（シャープ）」キー、「メモ／文字」キー、「F（ファンクション）」キーおよび「クリア」キーの各種キーが配列されてなるキー操作部3、通信時間や発信者電話番号などが表示されるディスプレイ4、マイク5ならびにスピーカ6が設けられている。また、筐体2の上部側にはアンテナケース部2aが筐体2に一体に設けられており、そのアンテナケース部2aの内部にはアンテナ7（図3参照）が配設されている。

【0017】次に、上述した携帯電話装置1の電気的な構成について、図3を参照して説明する。制御回路8（本発明でいう制御手段）は、マイクロコンピュータを主体として構成されており、この制御回路8には、音声処理部9、データ変換部10、送受信部11（本発明でいう送信手段、受信手段）、キー操作検出部12（本発明でいうキー操作検出手段）、表示制御部13、メモリ14（本発明でいう所定情報格納手段）が接続されている。音声処理部9は、上述したマイク5ならびにスピーカ6に接続されていると共に、データ変換部10に接続

されており、そのデータ変換部10は、送受信部11に接続され、その送受信部11には、上述したアンテナ7が接続されている。また、キー操作検出部12は、上述したキー操作部3に接続されており、表示制御部13は、上述したディスプレイ4に接続されている。

【0018】キー操作検出部12は、キー操作部3にあって各種キーが操作されると、そのキー操作に応じたキー操作検出信号を制御回路8に出力するようになっており、制御回路8は、キー操作検出部12からキー操作検出信号が与えられると、その与えられたキー操作検出信号に応じた処理を実行するようになっている。表示制御部13は、制御回路8から表示制御信号が与えられると、その与えられた表示制御信号に応じた表示内容をディスプレイ4に表示させるようになっている。

【0019】メモリ14は、音声情報格納領域、メモリダイヤル情報格納領域および電子メール情報格納領域を備えて構成されている。音声情報格納領域には、伝言メモ機能が動作することに応じて、発信者側から送信された音声情報が格納可能になっており、メモリダイヤル格納領域には、電話番号と、その電話番号に対応した名前が格納可能になっている。

【0020】また、この携帯電話装置1は、電子メールの送受信機能を備えているものであり、インターネットに接続されることによって、例えばパーソナルコンピュータとの間で電子メールを送受信することができるようになっている。そして、このとき、発信者側から送信された電子メール情報は、上記メモリ14の電子メール情報格納領域に格納されるようになっている。尚、ここでいうインターネットとは、企業、教育機関、その他の団体などのコンピュータネットワークが相互接続されたネットワークのことを総称しているものであり、また、場合によっては、NIFTY-Serve、PC-VANおよび日経MIXなどのパソコン通信網をも含んでいるものである。そして、制御回路8は、記憶されているプログラムを実行することによって、詳しくは後述する処理を実行するようになっている。

【0021】次に、上記構成の作用について、図1および図4～図7を参照して説明する。図1において、パーソナルコンピュータ（以下、パソコンと略称する）15は、モデムもしくはターミナルアダプタなどによって構成される通信機能を有しているもので、つまり、本発明でいう無線通信機能を有する装置である。そして、パソコン15と携帯電話装置1とは、通信網16を介して通信可能に構成されている。尚、ここで、通信網16とは、ISDN公衆回線やアナログ公衆回線などにより構成される電話通信網に加えて、インターネットを含んで構成される電子メール通信網をも総称するものである。また、携帯電話装置1は、電源が投入されている状態にあるものとする。

【0022】まず、パソコン15と携帯電話装置1とが

通信状態にあるときに、使用者がパソコン15を操作し、携帯電話装置1を遠隔操作するための所定の操作、例えば、遠隔操作番号として割当てられている「#」、「0」、「0」、「0」を入力すると、パソコン15は、その遠隔操作番号が格納された遠隔操作識別信号を送信させる(図1中、a参照)。パソコン15から送信された遠隔操作識別信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、遠隔操作処理に移行し、暗証番号要求信号を送信させる(図1中、b参照)。そして、携帯電話装置1の制御回路8は、これ以降、暗証番号を受信待機する。

【0023】携帯電話装置1から送信された暗証番号要求信号が通信網16を介してパソコン15に受信されると、パソコン15は、暗証番号の入力画面をディスプレイに表示させる。これによって、使用者は、次の動作、つまり、暗証番号を入力することが可能となる。

【0024】次いで、使用者が暗証番号として割当てられた数字を入力すると、パソコン15は、暗証番号が格納された暗証番号識別信号を送信させる(図1中、c参照)。パソコン15から送信された暗証番号識別信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、受信された暗証番号を識別し、識別結果が良好(正常)であるときには、認証OK信号を送信させる(図1中、d参照)。そして、携帯電話装置1の制御回路8は、これ以降、制御信号を受信待機する。

【0025】そして、携帯電話装置1から送信された認証OK信号が通信網16を介してパソコン15に受信されると、パソコン15は、制御指示の入力画面をディスプレイに表示させる。これによって、使用者は、次の動作、つまり、制御指示を入力することが可能となる。

【0026】さて、ここで、制御指示とは、具体的には、キー操作無効化指示、電源供給停止指示、音声情報読出指示、メモリダイヤル情報読出指示および電子メール情報読出指示であり、使用者は、これらのうちから任意のものを選択することができる。

【0027】まず、使用者が制御指示としてキー操作無効化指示を選択した場合について説明する。使用者が制御指示としてキー操作無効化指示を入力すると、パソコン15は、制御信号としてキー操作無効化信号を送信させる(図1中、e参照)。パソコン15から送信されたキー操作無効化信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、制御信号に応じた制御を実行し、この場合であれば、これ以降、携帯電話装置1におけるキー操作に対する処理を無効化し、応答信号を送信させる(図1中、f参照)。

【0028】そして、携帯電話装置1から送信された応答信号が通信網16を介してパソコン15に受信されると、パソコン15は、応答内容、この場合であれば、これ以降、携帯電話装置1におけるキー操作に対する処理

が無効化されることをディスプレイに表示させる。これによって、使用者は、その旨を認識することが可能となる。

【0029】このように、携帯電話装置1は、キー操作無効化信号を受信すると、これ以降、キー操作が実行されても、そのキー操作に対する処理を実行しなくなるように構成されているもので、つまり、使用者は、パソコン15を操作し、キー操作無効化信号を送信させることによって、携帯電話装置1におけるキー操作を無効化することができるものである。尚、この場合、キー操作に対する処理の禁止は、携帯電話装置1における電源の供給開始および供給停止に拘らず、継続して有効となるものである。

【0030】また、使用者が制御指示として電源供給停止指示を入力すると、パソコン15は、制御信号として電源供給停止信号を送信させる(図1中、e参照)。パソコン15から送信された電源供給停止信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、制御信号に応じた制御を実行し、この場合であれば、これ以降、携帯電話装置1における電源の供給を停止させ、応答信号を送信させる(図1中、f参照)。

【0031】そして、携帯電話装置1から送信された応答信号が通信網16を介してパソコン15に受信されると、パソコン15は、応答内容、この場合であれば、携帯電話装置1において電源の供給が停止されたことをディスプレイに表示させる。これによって、使用者は、その旨を認識することが可能となる。

【0032】このように、携帯電話装置1は、電源供給停止信号を受信すると、これ以降、電源の供給が停止されるように構成されているもので、つまり、使用者は、パソコン15を操作し、電源供給停止信号を送信させることによって、携帯電話装置1における電源の供給を停止させることができるものである。

【0033】さて、以上は、使用者が制御指示としてキー操作無効化指示および電源供給停止指示を選択した場合、つまり、制御信号がキー操作無効化信号および電源供給停止信号である場合について説明したものであるが、次に、使用者が制御指示として音声情報読出指示、メモリダイヤル情報読出指示および電子メール情報読出指示を選択した場合について、図4を参照して説明する。

【0034】まず、使用者が制御指示として音声情報読出指示を選択した場合について説明する。使用者が制御指示として音声情報読出指示を入力すると、パソコン15は、制御信号として音声情報読出信号を送信させる(図4中、g参照)。パソコン15から送信された音声情報読出信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、メモリ14の音声情報格納領域に音声情報が格納されている場合

には、その音声情報を読み出し、その音声情報が格納された音声情報信号を送信させる（図4中、h参照）。

【0035】そして、携帯電話装置1から送信された音声情報信号が通信網16を介してパソコン15に受信されると、パソコン15は、スピーカを備えている場合には、そのスピーカから音声情報を出力する。

【0036】このように、携帯電話装置1は、音声情報読出信号を受信すると、音声情報を読み出し、その音声情報が格納された音声情報信号を送信させるように構成されているもので、つまり、使用者は、パソコン15を操作し、音声情報読出信号を送信させることによって、携帯電話装置1に格納されている音声情報を読出すことができるものである。

【0037】また、使用者が制御指示としてメモリダイヤル情報読出指示を入力すると、パソコン15は、制御信号としてメモリダイヤル情報読出信号を送信させる（図4中、g参照）。パソコン15から送信されたメモリダイヤル情報読出信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、メモリ14のメモリダイヤル情報格納領域にメモリダイヤル情報が格納されている場合には、そのメモリダイヤル情報を読み出し、そのメモリダイヤル情報が格納されたメモリダイヤル情報信号を送信させる（図4中、h参照）。

【0038】そして、携帯電話装置1から送信されたメモリダイヤル情報信号が通信網16を介してパソコン15に受信されると、パソコン15は、ディスプレイにメモリダイヤル情報を出力する（表示する）。

【0039】このように、携帯電話装置1は、メモリダイヤル情報読出信号を受信すると、メモリダイヤル情報を読み出し、そのメモリダイヤル情報が格納されたメモリダイヤル情報信号を送信させるように構成されているもので、つまり、使用者は、パソコン15を操作し、メモリダイヤル情報読出信号を送信させることによって、携帯電話装置1に格納されているメモリダイヤル情報を読出すことができるものである。

【0040】さらに、使用者が制御指示として電子メール情報読出指示を入力すると、パソコン15は、制御信号として電子メール情報読出信号を送信させる（図4中、g参照）。パソコン15から送信された電子メール情報読出信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、メモリ14の電子メール情報格納領域に電子メール情報が格納されている場合には、その電子メール情報を読み出し、その電子メール情報が格納された電子メール情報信号を送信させる（図4中、h参照）。

【0041】そして、携帯電話装置1から送信された電子メール情報信号が通信網16を介してパソコン15に受信されると、パソコン15は、ディスプレイに電子メール情報を出力する（表示する）。

【0042】このように、携帯電話装置1は、電子メール情報読出信号を受信すると、電子メール情報を読み出し、その電子メール情報が格納された電子メール情報信号を送信させるように構成されているもので、つまり、使用者は、パソコン15を操作し、電子メール情報読出信号を送信させることによって、携帯電話装置1に格納されている電子メール情報を読み出すことができるものである。

【0043】以上に説明したように、使用者は、携帯電話装置1が手元に存在しない場合であっても、パソコン15が存在する環境であれば、パソコン15を操作することによって、携帯電話装置1におけるキー操作に対する処理を無効化したり、電源の供給を停止させたり、さらには、メモリ14に格納されている音声情報、メモリダイヤル情報および電子メール情報を読み出したりすることができるなど、携帯電話装置1を遠隔操作することができるものである。

【0044】ところで、携帯電話装置1は、上述したように制御信号を受信する機能を有しており、制御信号を受信すると、制御指示にしたがって遠隔操作されることが可能であるが、これに加えて、制御信号を送信する機能をも有しており、制御信号を送信することによって、他の携帯電話装置17（図5および図6参照）を遠隔操作することも可能に構成されている。

【0045】すなわち、使用者が携帯電話装置1を操作し、携帯電話装置17を遠隔操作するための遠隔操作番号として割当てられている例えば「#」キー、「0」キー、「0」キー、「0」キー、「0」キーを操作すると、携帯電話装置1の制御回路8は、キー操作が実行されたことを受けて、遠隔操作識別信号を送信させる（図5および図6中、i参照）。携帯電話装置1から送信された遠隔操作識別信号が通信網16を介して携帯電話装置17に受信されると、携帯電話装置17の制御回路8は、遠隔操作処理に移行し、暗証番号要求信号を送信させる（図5および図6中、j参照）。

【0046】そして、携帯電話装置17から送信された暗証番号要求信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、表示制御部13に表示制御信号を出力することによって、暗証番号の入力画面をディスプレイ4に表示させる。これによって、使用者は、次の動作、つまり、暗証番号を入力することが可能となる。

【0047】次いで、使用者が暗証番号として割当てられたキーを操作すると、携帯電話装置1の制御回路8は、キー操作が実行されたことを受けて、暗証番号識別信号を送信させる（図5および図6中、k参照）。携帯電話装置1から送信された暗証番号識別信号が通信網16を介して携帯電話装置17に受信されると、携帯電話装置17の制御回路8は、受信された暗証番号を識別し、識別結果が良好（正常）であるときには、認証OK

信号を送信させる（図5および図6中、1参照）。

【0048】そして、携帯電話装置17から送信された認証OK信号が通信網16を介して携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、表示制御部13に表示制御信号を出力することによって、制御指示の入力画面をディスプレイ4に表示させる。これによって、使用者は、次の動作、つまり、制御指示を入力することが可能となる。

【0049】次いで、使用者が制御指示として割当てられたキーを操作すると、携帯電話装置1の制御回路8は、キー操作が実行されたことを受けて、制御信号、つまり、上述したキー操作無効化信号、電源供給停止信号、音声情報読出信号、メモリダイヤル情報読出信号および電子メール情報読出信号のうちのいずれかを送信させる（図5中、m参照および図6中、o参照）。

【0050】そして、携帯電話装置1から送信された制御信号が通信網16を介して携帯電話装置17に受信されると、携帯電話装置17の制御回路8は、制御信号に応じた制御を実行し、また、制御信号がキー操作無効化信号、電源供給停止信号である場合には、応答信号を送信させ（図5中、n参照）、一方、制御信号が音声情報読出信号、メモリダイヤル情報読出信号、電子メール情報読出信号である場合には、音声情報信号、メモリダイヤル読出信号、電子メール情報信号を送信させる（図6中、p参照）。

【0051】そして、携帯電話装置1の制御回路8は、携帯電話装置17から送信された音声情報信号を受信したときには、音声情報をスピーカ6から出力し、メモリダイヤル情報信号を受信したときには、メモリダイヤル情報をディスプレイ4に出力し（表示し）、電子メール情報信号を受信したときには、電子メール情報をディスプレイ4に出力する（表示する）。

【0052】以上に説明したように、使用者は、上述したパソコン15を操作する代わりに、携帯電話装置1を操作することによっても、他の携帯電話装置17におけるキー操作に対する処理を無効化したり、電源の供給を停止させたり、さらには、メモリ14に格納されている音声情報、メモリダイヤル情報および電子メール情報を読出したりすることができるなど、他の携帯電話装置17を遠隔操作することができるものである。

【0053】尚、上述したパソコン15と携帯電話装置1との間で送受信される各種信号および携帯電話装置1と携帯電話装置17との間で送受信される各種信号は、例えば、図7に示すように、社団法人電波産業会（ARIB）のRCR-STD27Fにより規定されているユーザ・ユーザ情報転送付加サービスを利用することによって、トランスペアレントに送受信されることが実現できるものである。すなわち、ユーザ・ユーザ情報転送付加サービスでは、ユーザAとユーザBとの間で、ユーザ・ユーザ情報をトランスペアレントに送受信することが

可能であることから、各種信号をユーザ・ユーザ情報として送受信すれば良いものである。

【0054】また、携帯電話装置1および携帯電話装置17は、遠隔操作される場合には、通信状態であることが前提となるものであるが、この場合、例えば、あらかじめ伝言メモ機能を有効に設定しておくことによって、自動着信することが可能となり、通信状態となることが可能となる。

【0055】このように本実施例によれば、パソコン15から制御信号が送信され、その制御信号が携帯電話装置1に受信されると、携帯電話装置1の制御回路8は、制御信号に応じた制御を実行するようになるので、使用者は、仮に、携帯電話装置1が手元に存在しない場合でも、パソコン15が存在する環境であれば、そのパソコン15を操作し、パソコン15から制御信号を送信させることによって、携帯電話装置1に制御信号に応じた処理を実行させることができる。具体的には、携帯電話装置1におけるキー操作を無効化したり、電源の供給を停止させたり、さらには、メモリ14に格納されている音声情報、メモリダイヤル情報および電子メール情報を読出すことができる。このように、パソコン15を操作することによって、携帯電話装置1を遠隔操作することができるので、利便性の向上を図ることができる。

【0056】また、キー操作検出部3により所定のキー操作がなされたことが検出されると、携帯電話装置1の制御回路8は、制御信号を送信させるようになるので、使用者は、携帯電話装置1を操作し、携帯電話装置1から制御信号を送信させることによって、他の携帯電話装置17において制御信号に応じた処理を実行させることができる。このように、パソコン15を操作する代わりに、携帯電話装置1を操作することによっても、他の携帯電話装置17を遠隔操作することができるので、利便性の向上をより図ることができる。

【0057】また、携帯電話装置1の制御回路8および携帯電話装置17の制御回路8は、パソコン15や他の携帯電話装置から送信された暗証番号の識別結果が良好（正常）であることを条件として、制御信号に応じた制御を実行するようになるので、使用者は、暗証番号を送信させることによってのみ、制御信号に応じた制御を実行させることができ、つまり、第三者の操作によって、制御信号に応じた制御が実行されることを防止することができ、利便性の向上をより図ることができ、場合によっては、秘匿性の向上をも図ることができる。

【0058】本発明は、上記した実施例にのみ限定されるものでなく、次のように変形または拡張することができる。無線通信装置としては携帯電話装置に限らず、簡易型携帯電話装置（PHS：Personal Handyphone System）などの他のものであっても良い。

【0059】キー操作を無効化したり（ダイヤルロック）、電源の供給を停止させたりすることに限らず、発

信動作を禁止したり（ダイヤル発信禁止）、さらには、メモリに格納されている情報の読出動作を禁止したり（メモリ使用禁止）するようにしても良い。無線通信機能を有する装置としては、パソコンや携帯電話装置に限らず、PDA（Personal Digital Assistant）端末などであっても良い。

【図面の簡単な説明】

【図1】本発明の一実施例を示すシーケンス図

【図2】正面外観図

【図3】電気的構成を示すブロック構成図

【図4】図1相当図

*【図5】図1相当図

【図6】図1相当図

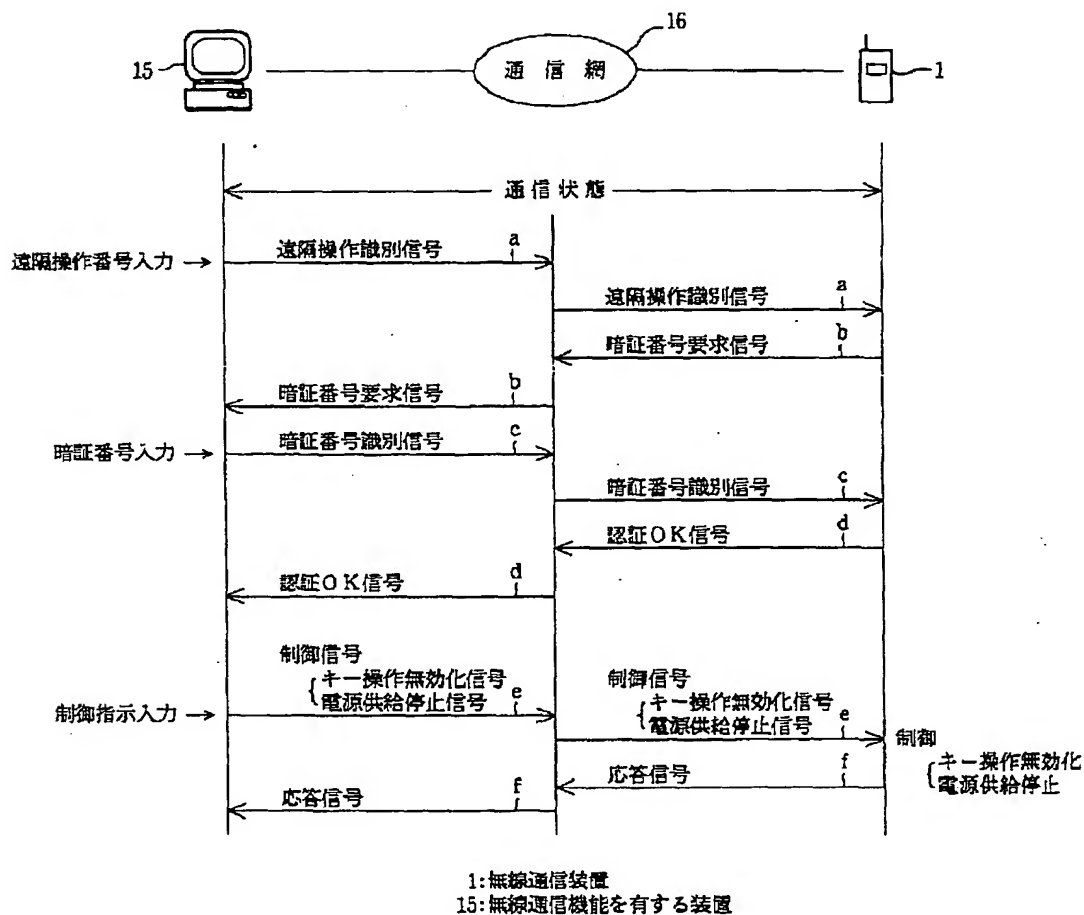
【図7】ユーザ・ユーザ情報転送付加サービスのシーケンス図

【符号の説明】

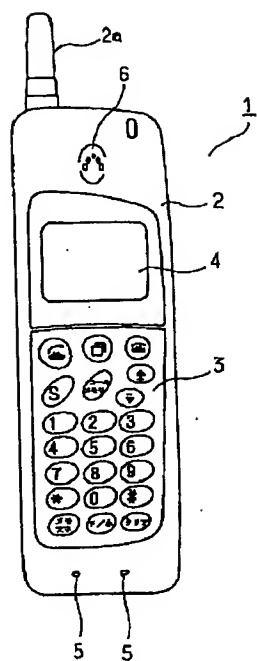
図面中、1は携帯電話装置（無線通信装置）、8は制御回路（制御手段）、11は送受信部（送信手段、受信手段）、12はキー操作検出部（キー操作検出手段）、14はメモリ（所定情報格納手段）、15はパーソナルコンピュータ（無線通信機能を有する装置）、17は携帯

電話装置（無線通信装置）である。

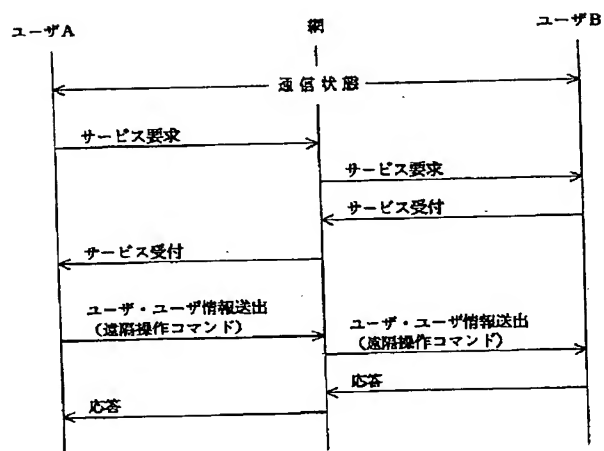
【図1】



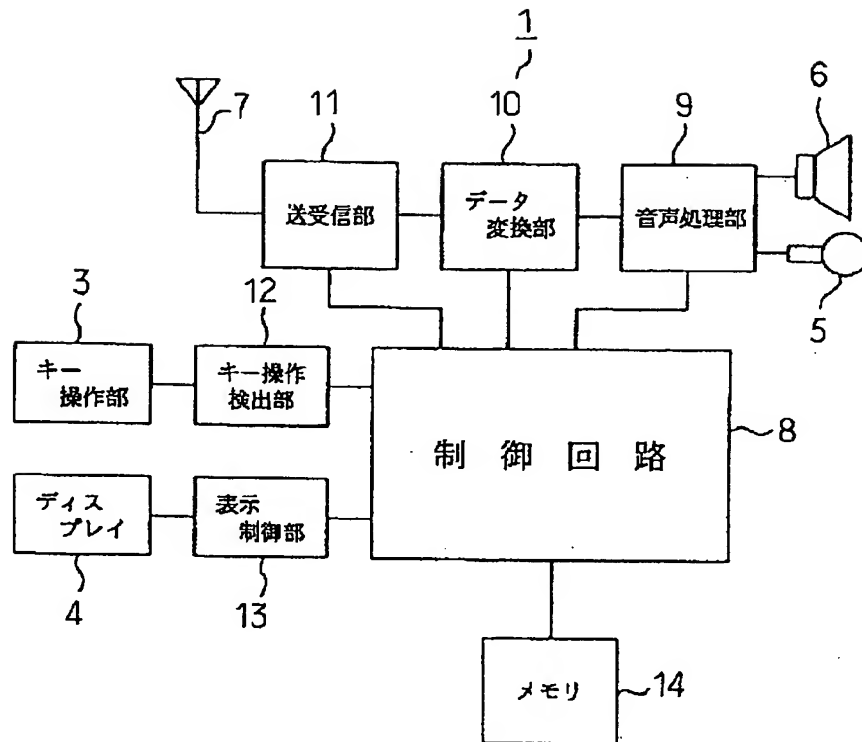
【図2】



【図7】

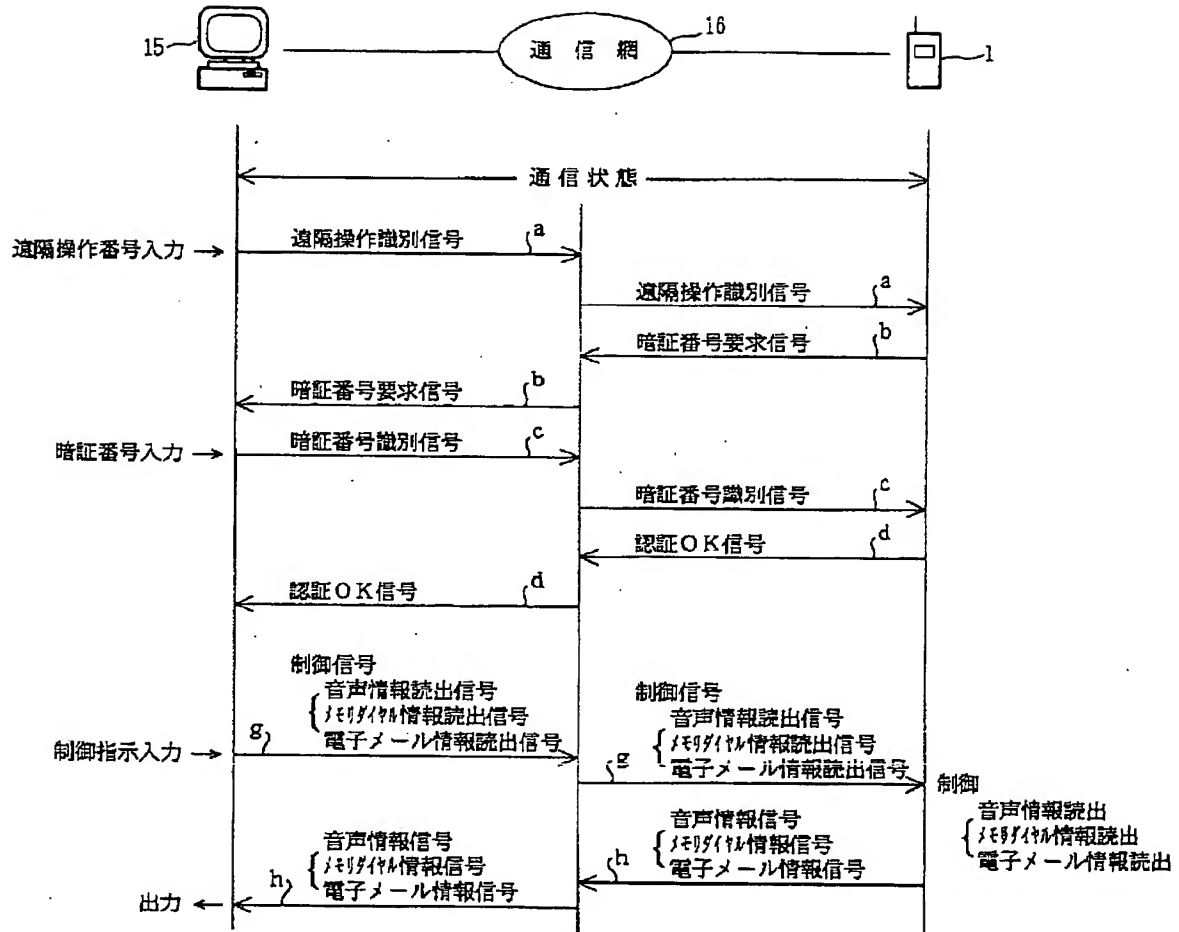


【図3】



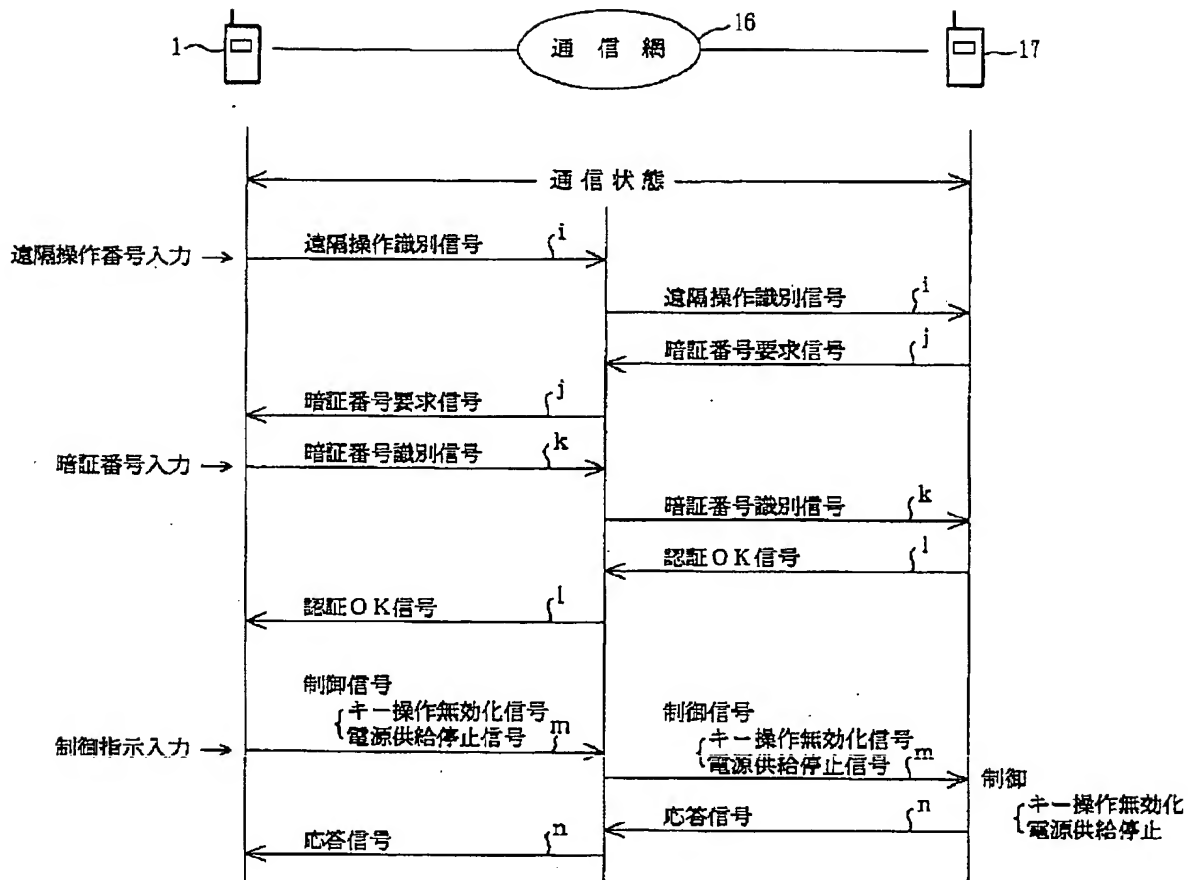
- 8: 制御手段
- 11: 送信手段、受信手段
- 12: キー操作検出手段
- 14: 所定情報格納手段

【図4】



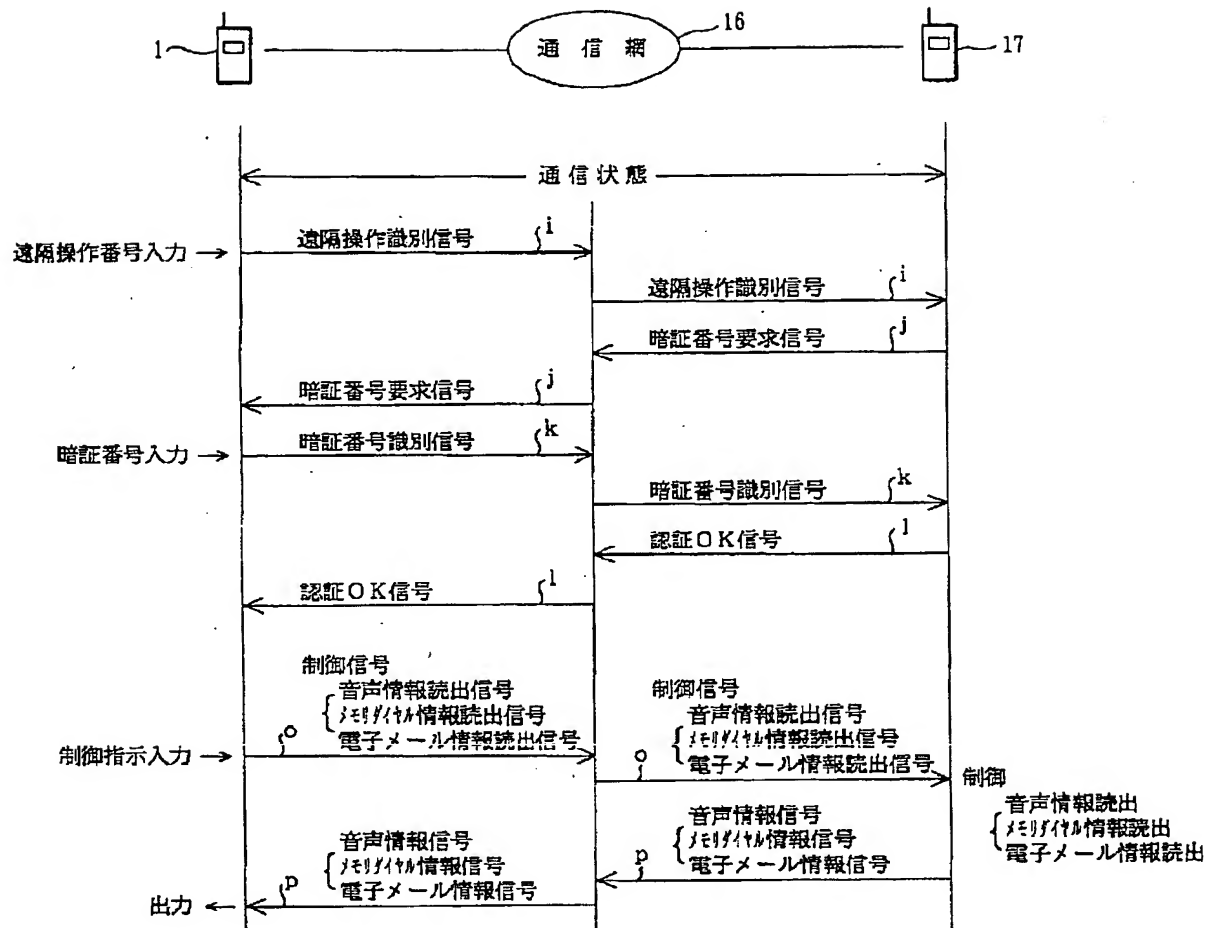
10

【図5】





【図6】







PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07226732 A**(43) Date of publication of application: **22.08.95**

(51) Int. Cl. **H04L 9/00**
H04L 9/10
H04L 9/12
G09C 1/00
H04Q 7/38

(21) Application number: **06017687**(22) Date of filing: **14.02.94**(71) Applicant: **FUJITSU LTD**

(72) Inventor: **TORII NAOYA**
AKIYAMA RYOTA
TAKENAKA MASAHIKO

(54) **COMMUNICATION TERMINAL EQUIPMENT
 VERIFICATION DEVICE**

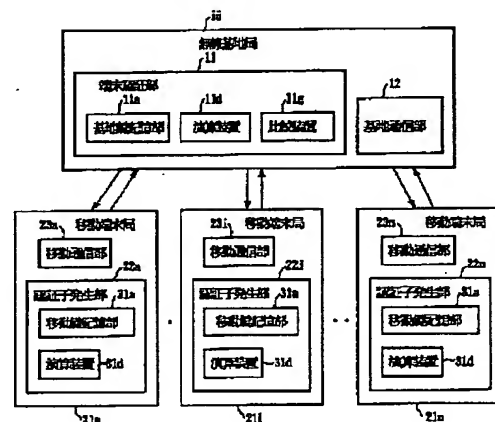
random number string to obtain the 2nd authenticator.

COPYRIGHT: (C)1995,JPO

(57) Abstract:

PURPOSE: To secure the confidentiality of a secret key by devising the verification equipment such that decoding of the secret key by an intercept party is more difficult.

CONSTITUTION: A base key storage section 11a and a mobile key storage section 31a store plural kinds of secret keys corresponding to plural kinds of key indices for each mobile terminal equipment station. An arithmetic unit 11d calculates an inner produce between a secret key and a random number string to obtain a 1st authenticator, a comparator 11g compares the 1st authenticator with a 2nd authenticator to provide a prescribed enable signal, a base communication section 12 sends a random number string and a key index and receives the 2nd authenticator. A mobile communication section 23 receives the random number string and the key index and sends the 2nd authenticator and the arithmetic unit 31d extracts the secret key corresponding to the key index received from the base communication section 12 from the mobile key storage section and calculates an inner product between the secret key and the received



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平7-226732

(43)公開日 平成7年(1995)8月22日

(51)Int.Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/00

9/10

9/12

H 0 4 L 9/ 00

Z

7605-5K

H 0 4 B 7/ 26

1 0 9 S

審査請求 未請求 請求項の数5 OL (全 14 頁) 最終頁に続く

(21)出願番号 特願平6-17687

(22)出願日 平成6年(1994)2月14日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72)発明者 鳥居 直哉

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72)発明者 秋山 良太

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72)発明者 武仲 正彦

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

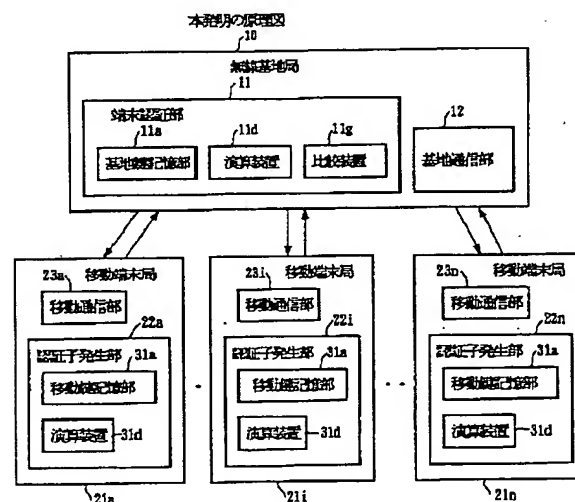
(74)代理人 弁理士 遠山 勉 (外1名)

(54)【発明の名称】 通信端末認証装置

(57)【要約】

【目的】秘密鍵の機密性を保持する。

【構成】基地鍵記憶部11a及び移動鍵記憶部31aは移動端末局毎に複数種類の鍵インデックスに対応付けて複数種類の秘密鍵を記憶する。演算装置11dは秘密鍵と乱数列との内積を演算して第1の認証子を求め、比較装置11gは第1の認証子と第2の認証子とを比較して所定の許可信号を出力し、基地通信部12は乱数列と鍵インデックスとを送信すると共に第2の認証子を受信する。移動通信部23は乱数列と鍵インデックスとを受信すると共に第2の認証子を送信し、演算装置31dは基地通信部12から受信した鍵インデックスに対応する秘密鍵を移動鍵記憶部から取り出し秘密鍵と受信した乱数列との内積を演算して第2の認証子を求める。



【特許請求の範囲】

【請求項 1】 無線基地局（10）と移動端末局（21i）との間で通信許可を付与するための認証を行う通信端末認証装置であって、

前記無線基地局（10）は、前記移動端末局毎に複数種類の秘密鍵（Ksi）と複数種類の秘密鍵の各々を指定する複数種類の鍵インデックス（IKi）とを対応付けた基地鍵記憶部（11a）と、前記秘密鍵と予め定められた乱数列（Ri）との内積を演算して第 1 の認証子

（MS1i）を求める演算装置（11d）と、求められ 10
た第 1 の認証子と第 2 の認証子（MS2i）とを比較して所定の許可信号を出力する比較装置（11g）とを有する端末認証部（11）と、

前記乱数列と鍵インデックスとを送信するとともに前記第 2 の認証子を受信する基地通信部（12）とを備え、前記移動端末局（21i）は、前記乱数列と鍵インデックスとを受信するとともに前記第 2 の認証子を送信する移動通信部（23）と、

前記移動端末局毎に前記複数種類の秘密鍵と前記複数種類の鍵インデックスとを対応付けた移動鍵記憶部（31a）と、前記基地通信部（12）から受信した鍵インデックスに対応する秘密鍵を前記移動鍵記憶部から取り出しこの秘密鍵と受信した乱数列との内積を演算して前記第 2 の認証子を求める演算装置（31d）とを有する認証子発生部（22）とを備えたことを特徴とする通信端末認証装置。 20

【請求項 2】 請求項 1 において、前記端末認証部（11）は、前記秘密鍵と乱数列との内積を演算して求めた後に、秘密鍵に基づく位置から所定の長さのデータを前記第 1 の認証子とすることを特徴とする通信端末認証装置。 30

【請求項 3】 請求項 1 において、前記端末認証部（11）は、前記秘密鍵と前記乱数列との内積を演算して求めた後に、前記秘密鍵に基づいて転置処理を行ったデータを前記第 1 の認証子とすることを特徴とする通信端末認証装置。

【請求項 4】 請求項 1 において、前記端末認証部（11）は、前記秘密鍵に基づいて前記乱数列を転置処理した後に、前記秘密鍵との内積を演算して求めたデータを前記第 1 の認証子とすることを特徴とする通信端末認証装置。 40

【請求項 5】 請求項 1 において、前記端末認証部（11）は、鍵インデックスが変わる毎に前記秘密鍵に対して異なる転置を行うことを特徴とする通信端末認証装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、無線通信局間の通信端末認証装置に関し、特に無線基地局と移動端末局との間で通信許可を付与するための認証を行う通信端末認証装 50

置に関する。

【0002】

【従来の技術】 近年、人、自動車などの移動体による移動通信が実用化されてきた。この移動通信では、任意の場所で通信を行えるという利点がある。特に、自動車電話や携帯電話機等の普及により高度のサービスが提供されつつある。

【0003】 このような移動通信は、移動端末局と無線基地局（センタ局ともいう。）との間で行なわれる。移動端末局は移動体に無線通信設備を備えた端末装置であり、無線基地局は移動端末局を管理する。

【0004】 この移動端末局と無線基地局との間で無線通信を行う場合に、通信接続を希望する移動端末局が無線基地局に登録されている正規の移動端末局であるか否かを判別する必要がある。

【0005】 この判別によって移動端末局の正当性を証明することを認証と呼ぶ。そして、移動無線局は認証を受けるために無線基地局へ移動端末局毎に付された固有の ID（Identity）と呼ばれる識別符号を送送する。

【0006】 この識別符号が、他の無線機器等によって傍受されても、その内容が分からないようにするためにデータの暗号化処理を行って伝送していた。従来では、データの暗号化処理として、例えば DES（Data Encryption Standard）方式を用いていた。この DES 方式は同一の鍵または一方から他方が容易に導ける鍵の対を用いる暗号方式である共通鍵方式（Common key system）の一つであって、乱数、換字及び転置を複雑に組み合わせた方式である。この換字は鍵によって指定された方法で文字を他の文字で置き換えるものであり、転置は文字の順序を入れ換えるものである。

【0007】 この DES 方式では、64 ビットの単位で変換が行われる。そして、正規の移動端末局では、予め定められた前記乱数を用いて、換字、転置を行うことによりデータの復号化を行っていた。

【0008】

【発明が解決しようとする課題】 しかしながら、従来の DES 方式にあっては、複雑なアルゴリズムを用いているため、ソフトウェアで実行するには処理時間を要していた。また、ハードウェアで実現するには、端末装置の容量の上で問題があった。

【0009】 本発明は、このような点に鑑みてなされたもので、その目的とするところは、簡便なマイクロコントローラでも容易に実現可能であって、かつ秘密鍵を容易に解読できることなく、秘密鍵の機密性を十分に保持することのできる通信端末認証装置を提供することにある。

【0010】

【課題を解決するための手段】 本発明は、前記課題を解決するために下記の構成とした。図 1 は本発明の原理図である。図 1 に従って、本発明を説明する。

【0011】本発明の通信端末認証装置は、無線基地局10と移動端末局21iとの間で通信許可を付与するための認証を行う。前記無線基地局10は、端末認証部11、基地通信部12とを備える。端末認証部11は、基地鍵記憶部11a、演算装置11d、比較装置11gを有する。

【0012】基地鍵記憶部11aは前記移動端末局毎に複数種類の鍵インデックスIKiに対応付けて複数種類の秘密鍵Ksiを記憶する。演算装置11dは秘密鍵と予め定められた乱数列Riとの内積を演算して第1の認証子MS1iを求める。

【0013】比較装置11gは求められた第1の認証子と第2の認証子MS2iとを比較して所定の許可信号を出力する。基地通信部12は前記乱数列と鍵インデックスとを送信するとともに前記第2の認証子を受信する。

【0014】前記移動端末局21iは、移動通信部23、認証子発生部22とを備える。認証子発生部22は移動鍵記憶部31a、演算装置31dを備える。移動通信部23は前記乱数列と鍵インデックスとを受信するとともに前記第2の認証子を送信する。

【0015】移動鍵記憶部31aは、前記移動端末局毎に前記複数種類の鍵インデックスに対応付けて複数種類の秘密鍵を記憶する。演算装置31dは前記基地通信部12から受信した鍵インデックスに対応する秘密鍵を前記移動鍵記憶部から取り出しこの秘密鍵と受信した乱数列との内積を演算して前記第2の認証子を求める。

【0016】ここで、前記端末認証部11は、前記秘密鍵と乱数列との内積を演算して求めた後に、秘密鍵に基づく位置から所定の長さのデータを前記第1の認証子としてもよい。なお、前記認証子発生部22は、前記秘密鍵と乱数列との内積を演算して求めた後に、秘密鍵に基づく位置から所定の長さのデータを前記第2の認証子としてもよい。

【0017】また、前記端末認証部11は、前記秘密鍵と前記乱数列との内積を演算して求めた後に、前記秘密鍵に基づいて転置処理を行ったデータを前記第1の認証子としてもよい。なお、前記認証発生部22は、前記秘密鍵と前記乱数列との内積を演算して求めた後に、前記秘密鍵に基づいて転置処理を行ったデータを前記第2の認証子としてもよい。

【0018】さらに、前記端末認証部11は、前記秘密鍵に基づいて前記乱数列を転置処理した後に、前記秘密鍵との内積を演算して求めたデータを前記第1の認証子としてもよい。なお、前記認証発生部22は、前記秘密鍵に基づいて前記乱数列を転置処理した後に、前記秘密鍵との内積を演算して求めたデータを前記第2の認証子としてもよい。

【0019】また、前記端末認証部11は、鍵インデックスが変わる毎に前記秘密鍵に対して異なる転置を行うようにしてもよい。あるいは、秘密鍵に対して論理和、

論理積、換字、それらの組み合わせ処理を行うようにしてもよい。

【0020】さらに、秘密鍵を用いて内積処理に対する前処理あるいは後処理として複数の変換処理を用意し、複数の変換処理のいずれかを選択して処理を行うようにしてもよい。複数の変換処理としては、例えば論理和、論理積、排他的論理和、換字、それらの組み合わせ処理である。

【0021】このような処理を行うことで、さらに、秘密鍵の解読が困難になるため、秘密鍵の機密性が保持できる。

【0022】

【作用】本発明によれば、無線基地局10において、端末認証部11では、複数種類の秘密鍵の内、記鍵インデックスに対応する一の秘密鍵が基地鍵記憶部11aから読み出される。そして、この鍵インデックスと乱数列Riとを基地通信部12が送信される。

【0023】次に、移動端末局21iにおいて、移動通信部23が前記鍵インデックスIKiと乱数列Riとを受信すると、鍵インデックスIKiに対応する秘密鍵が移動鍵記憶部31aから読み出される。そして、演算装置31dがこの秘密鍵と受信した乱数列との内積を演算して第2の認証子を求め、移動通信部23が第2の認証子を送信する。

【0024】さらに、無線基地局10において、基地通信部12が第2の認証子を受信する。演算装置11dは、前記秘密鍵と出力された前記乱数列との内積を演算して第1の認証子MS1iを求め、比較装置11gは求められた第1の認証子と第2の認証子MS2iとを比較して所定の許可信号を出力する。

【0025】すなわち、本発明では、移動端末局毎に複数種類の秘密鍵を有するとともに複数種類の秘密鍵のいずれかを鍵インデックスにより指定できるので、移動端末局毎に秘密鍵が1つの秘密鍵よりも複数種類増加するため、傍受者には秘密鍵の解読がより困難になる。従って、よりデータの秘密性を保持することができる。

【0026】

【実施例】以下、本発明の通信端末認証装置の実施例を説明する。図2は本発明の通信端末認証装置の実施例1の構成ブロック図である。

<実施例1>図2に示すように、通信端末認証装置は無線基地局10と複数の移動端末局21とからなり、無線基地局10と各移動端末局21(21a~21n)との間で無線通信を行う。

【0027】無線基地局10は端末認証部11、基地通信部12、制御部13とを備える。各移動端末局21(21a~21n)は認証子発生部22(22a~22n)、移動通信部23(23a~23n)、制御部24(24a~24n)を備える。

【0028】無線基地局10において、端末認証部11

10

20

30

40

50

は、通信接続可能な移動端末局21(21a~21n)毎に複数種類の秘密鍵Ksi(Ksi1, Ksi2... Ksin)(sは1以上mである。)と鍵インデックスIKi(s=IKi, IKiは1以上mである。)とを対応付けて鍵データベース11aに格納する。また、端末認証部11は、乱数列Ri(ri1, ri2... rin)(各要素は予め定められたビット幅をもつ。)を発生して移動端末局21(21a~21n)に出力する。

【0029】無線基地局10は、鍵インデックスIKi 10により指定された秘密鍵Ksi(Ksi1, Ksi2... Ksin)と出力した乱数列Ri(ri1, ri2... rin)との内積を演算して得られた第1の認証子MS1iと移動端末局21から受信した第2の認証子とを比較して通信許可信号または通信拒否信号を出力する。

【0030】基地通信部12は、乱数列Riと鍵インデックスIKiを送信するとともに、第2の認証子MS2iを受信する。制御部13は無線基地局10全体を制御するとともに、端末認証部11及び基地通信部12の動作を制御する。 20

【0031】なお、乱数列Ri及び秘密鍵は例えば、夫々512ビットの符号列であり、要素の長さは8ビットである。移動端末局21a~21nにおいて、移動通信部23a~23nは夫々乱数列Ri及び鍵インデックスIKiを受信するとともに、第2の認証子MS2iを送信す*

$$s = IKi$$

図4に鍵データベースに格納される複数種類の秘密鍵と鍵インデックスとの対応を示す。図4に示したように移動端末局21iに対して複数種類の鍵インデックスIKi 30(IK1i, IK2i... IKmi)と複数種類の秘密鍵Ksi(K1i, K2i... Kmi)とが対応している。

【0036】制御部13は鍵データベース11aからその鍵インデックスIKiに対応する秘密鍵Ksiを取り出す。乱数発生装置11bは、図2に示した制御部13からの指令に応じて、鍵インデックスIKiと例えば日付・時刻によって変化する乱数列Riを発生する。 ※

$$MSi = \sum Ksij \times rij$$

なお、jは1からnまで変化させる。

【0040】後処理装置11eは演算装置11dで得られた内積列MS1iについて、秘密鍵Ksiに基づき後★

$$Si = TKi(MSi)$$

ここで、TKi(MSi)はMSiの内、鍵で定められた位置のデータをSiとして取り出す関数である。すなわち、Siのビット長をNsとし、MSiのビット長をNmとする。このとき、NmはNsよりも大であり、Kiの値によりSiの取り出し位置を変更する。

【0042】例えば図5に認証子の決定方法の一例を示す。図5(a)に内積列MSiの例を示し、図5(b) 50

*る。認証子発生部22a~22nは、複数種類の秘密鍵Ksiの中の鍵インデックスIKiに対応する秘密鍵Ksiと受信した乱数列Riとの内積を演算して得られた第2の認証子MS2iを無線基地局10に出力する。

【0032】制御部24a~24nは、移動端末局21a~21n全体を制御するとともに、移動通信部23a~23n及び認証子発生部22a~22nの移動制御を行う。

【0033】次に、無線基地局10に設けられた端末認証子部11、及び移動端末局21に設けられた認証子発生部23の具体的な構成について説明する。図3は実施例1の端末認証部11の構成ブロック図である。端末認証部11は鍵データベース11a、乱数発生装置11b、出力装置11c、演算装置11d、後処理装置11e、入力装置11f、比較装置11g、各々の装置を制御する制御回路11hとを備える。

【0034】鍵データベース11aは通信可能な移動端末局21a~21i~21n毎に複数種類の秘密鍵Ksi(Ksi1, Ksi2... Ksin)と鍵インデックスIKi(s=IKi, IKiは1以上mである。)とを対応付けて格納する。ここで、iは任意の移動端末番号を示し、1以上nである。nは全ての端末数を示す。sは1以上mであるので、複数種類の秘密鍵Ksiは移動端末局毎にm種類用意される。

【0035】すなわち、数式で表すと、(1)式のようになる。

$$\dots (1)$$

※【0037】出力装置11cは、乱数発生装置11bで発生した乱数列Riと鍵インデックスIKi及び後述する比較装置11gから出力された所定の許可信号YNを一定の出力レベルに増幅して出力する。

【0038】演算装置11dは鍵データベース11aに格納された秘密鍵Ksiと、乱数発生装置11bで発生した乱数列Riとの内積を夫々演算して内積列MS1iを求める。

【0039】すなわち、数式で表すと、(2)式のようになる。

$$\dots (2)$$

40★処理を行い、第1の認証子S1iを求める。すなわち、数式で表すと、(3)式のようになる。

$$[0041]$$

$$\dots (3)$$

に鍵Kiと認証子Siとを対応付けたテーブル80を示す。ここでは、簡単のために内積列MSiを16ビット、認証子Siを8ビットとする。図5(a)において、内積列70は16ビットとし、鍵71は先頭の4ビットとする。

【0043】図5(b)に示すテーブル80では、鍵が「0000」である場合には、第1番目(上位1ビッ

ト)から8ビットまでの「10111110」が認証子 S_i となる。鍵が「0001」である場合には、第2番目から8ビットまでの「01111100」が認証子 S_i となる。

【0044】なお、認証子 S_i の決定方法として、前記とは逆に内積列の下位1ビットから順に選択するようにしてもよい。入力装置11fは基地通信部12によって受信した第2の認証子 S_2i を受ける。比較装置11gは後処理装置11eから出力された認証子 S_1i と、入力装置11fから出力された認証子 S_2i とを比較し、所定の許可信号YNを出力する。具体的には、認証子 S_1i と、入力装置11fから出力された認証子 S_2i とが一致した場合には通信許可信号を出力し、そうでない場合には通信拒否信号を出力する。

【0045】図6は実施例1の認証子発生部22aの構成ブロック図である。認証子発生部22b、22c・・・22nはいずれも同一構成であるので、ここでは認証子発生部22aの構成を説明する。

【0046】認証子発生部22aは、入力装置31f、演算装置31d、秘密鍵テーブル31a、後処理装置31e、及び出力装置31c、制御回路31hの各部から構成される。

【0047】入力装置31fは基地通信部12によって受信した乱数列R1を受ける。演算装置31dは前記(2)式を用いて秘密鍵 K_{si} と受信した乱数列R1との内積とを演算して内積列 MS_2i を求める。

【0048】秘密鍵テーブル31aは前記鍵データベース11aに格納された内容と同一の内容を格納している。すなわち、秘密鍵テーブル31aは移動端末局21毎に複数種類の秘密鍵 K_{si} と複数種類の秘密鍵 K_{si} の各々を指定する鍵インデックス IK_i ($s=IK_i$ 、 IK_i は1以上mである。)とを対応付けて格納する。この秘密鍵テーブル31aは前記図4に示すように複数種類の秘密鍵 K_{si} と鍵インデックス IK_i とを格納している。

【0049】後処理装置31eは演算装置31dで求められた内積列 MS_2i について、前記秘密鍵に基いて前記(3)式の同様な後処理を行い、認証子 MS_2i を求めて出力装置31cに出力する。

【0050】出力装置31cは後処理装置31eから出力された認証子 MS_2i を一定の出力レベルに増幅して無線基地局10に出力する。図7に実施例1の無線基地局10の処理フローチャートを示す。図7に示す処理フローを用いて無線基地局10の動作を説明する。まず、無線基地局10において、乱数発生装置11bが乱数R1と鍵インデックス IK_i を発生し(ステップ101)、乱数列R1と鍵インデックス IK_i とを出力装置11cで所定の出力レベルまで増幅する。そして、基地通信部12が乱数列R1と鍵インデックス IK_i とを各移動端末局21a～21nに送信する(ステップ10

2)。

【0051】次に、移動端末局21から送信されてくる第2の認証子 S_2i を受信する(ステップ103)。なお、移動端末局21で得られる第2の認証子については、移動端末局21の処理フローチャートで説明する。

【0052】さらに、秘密鍵データベース11aから通信すべき移動端末局21における複数種類の秘密鍵の内、鍵インデックス IK_i に対応する秘密鍵 K_{si} を取り出す(ステップ104)。そして、(2)式を用いて乱数列R1と取り出した秘密鍵 K_{si} との内積列 MS_2i を演算する(ステップ105)。なお、内積演算の詳細については後述する。

【0053】さらに、得られた内積列 MS_1i に基いて(3)式による抽出処理を行うことにより第1の認証子 S_1i を求める(ステップ106)。ステップ103で受信した移動端末局21の第2の認証子とステップ106で求められた第1の認証子との比較を行う。

【0054】移動端末局21が無線基地局10に正規に登録された端末局か否かを判別する(ステップ108)。すなわち、ステップ103で受信した移動端末局21の第2の認証子と、ステップ106で求められた第1の認証子とが一致するか否かを判別する。ここで、第1の認証子と第2の認証子とが一致する場合には、処理を終了する。そうでない場合には、ステップ101に戻る。

【0055】すなわち、移動端末局21毎に複数種類の秘密鍵 K_{si} を有するとともに複数種類の秘密鍵 K_{si} のいずれかを鍵インデックス IK_i により指定できるので、移動端末局毎に秘密鍵が1つの秘密鍵よりも複数種類増加するため、傍受者には秘密鍵の解読がより困難になる。従って、よりデータの秘密性を保持することができる。

【0056】図8に移動端末局の処理フローチャートを示す。まず、各移動端末局21a～21nでは、無線基地局10から送信された鍵インデックス IK_i と乱数列R1の受信を待つ(ステップ111)。そして、入力装置31fが鍵インデックス IK_i と乱数列R1を受信すると、演算装置31dは鍵インデックス IK_i に対応する秘密鍵 K_i を秘密鍵テーブル31aから取り出す(ステップ112)。

【0057】さらに、演算装置31dは、ステップ111で受けた乱数列R1とステップ112で取り出した秘密鍵とから(2)式を用いて内積を演算して、内積列 MS_2i を求める(ステップ113)。

【0058】次に、後処理装置31eはステップ113で求められた内積列 MS_2i に基いて抽出処理を行うことにより第2の認証子 S_2i を求める(ステップ114)。ステップ114で求められた第2の認証子を実無線基地局10に送信する(ステップ116)。

【0059】次に、前記内積演算処理及び後処理の具体

10

20

30

40

50

的な処理手順について説明する。図9に実施例1の内積処理フローチャートを示す。図9において、まず、変数 j 及び内積列 MS_i を初期化する。ここでは、変数 j に「1」を代入し、内積列 MS_i に「1」を代入する（ステップ121）。

【0060】次に、内積演算を行う。ここでは、秘密鍵 K_{si} の j 番目のビット (K_{sij}) と乱数列 r_i の j 番目のビット (r_{ij}) との内積に前記内積列 MS_i を加算したものを内積列 MS_i として代入する（ステップ122）。そして、変数 j の値を1だけインクリメントする（ステップ123）。

【0061】次に、変数 j の値が所定の数 ($n+1$) を越えたか否かを判別する（ステップ124）。ここで、変数 j が所定の数 ($n+1$) を越えた場合には内積処理を終了する。そうでない場合にはステップ122に戻る。

【0062】図10に実施例1の後処理フローチャートを示す。図10において、演算装置が秘密鍵テーブル31aから秘密鍵 K_{si} を取り出す（ステップ125）。次に、図5に示すようなテーブルを用いて内積列 MS_i の取り出し位置を秘密鍵 K_{si} の値により決定する（ステップ126）。すると、任意の位置の認証子 S_i が取り出される（ステップ127）。

<実施例2>次に、本発明の実施例2について説明する。実施例2では、実施例1の後処理における抽出処理に代えて、転置処理を行う点が異なる。

【0063】図11に実施例2の後処理フローチャートを示す。この場合には、後処理として転置処理を行うものとする。演算装置31dが秘密鍵テーブル31aから秘密鍵 K_{si} を取り出す（ステップ125）。そして、乱数列 R_i と鍵 K_{si} とから内積列 MS_i を演算した後、この鍵 K_i に基づき内積列 MS_i の転置処理を行う（ステップ128）。

【0064】すなわち、ステップ114で求められた内積列 MS に基いて認証子 S_i の転置処理を行う。例えば、図12に示すように、鍵が「000」である場合に転置前のデータ「 $A_1, A_2 \cdots A_n$ 」を転置後のデータ「 $A_n, A_1, A_2 \cdots A_{n-1}$ 」のように転置する。また、鍵が「010」である場合に転置前のデータ「 $A_3, A_1 \cdots A_n$ 」を転置後のデータ「 $A_1, A_3, A_2 \cdots A_n$ 」のように転置する。

【0065】このような転置処理を行うことで、秘密鍵の機密性が保持できる。

<実施例3>次に、本発明の実施例3について説明する。実施例3では、実施例1の後処理における抽出処理と実施例2の転置処理とを組み合わせたものである。

【0066】図13に実施例3の後処理フローチャートを示す。まず、演算装置が秘密鍵 K_{si} を取り出す（ステップ125）。次に、図12に示すように鍵に基づき内積列 MS_i の転置処理を行う（ステップ128）。50

【0067】すなわち、ステップ114で求められた内積列 MS に基いて認証子の転置処理を行う。さらに、内積列 MS_i の取り出し位置を秘密鍵 K_{si} から定めて取り出す（ステップ129）。

【0068】この場合には、転置処理と抽出処理とを行うことでさらに、秘密鍵が解読しにくくなり、秘密鍵の機密性が保持できる。

<実施例4>次に、本発明の実施例4について説明する。図14に実施例4の端末認証部の構成ブロック図を示す。実施例4では、端末認証部44において、乱数発生装置11bと演算装置11dとの間に前処理装置11jを備える点が実施例1に対して異なる。図14において、前処理装置11jは、鍵データベース11aから通信すべき移動端末局21における鍵インデックス IK_i に対応する秘密鍵 K_{si} を取り出して、秘密鍵 K_{si} と乱数発生装置11bから出力された乱数列 R_i との排他的論理和をとる。

【0069】図15に実施例4の認証子発生部の構成ブロック図を示す。実施例4では、認証子発生部54において、入力装置31fと演算装置31dとの間に前処理装置31jを備える点が実施例1に対して異なる。図15において、前処理装置31jは、前記秘密鍵テーブル31aからの秘密鍵と入力装置31fからの乱数列 R_i との排他的論理和をとる。

【0070】このような前処理装置11j、31jを用いるので、認証子等の符号列が傍受されても、排他的論理和処理によって、その内容を解析することはより困難となるので、通信内容の秘密性を確保することができ

る。

【0071】図16に実施例4の無線基地局の処理フローチャートを示す。このように構成された実施例4における無線基地局の処理を説明する。まず、無線基地局10において、乱数発生装置11bが乱数 R_i と鍵インデックス IK_i を発生し（ステップ401）、乱数列 R_i と鍵インデックス IK_i とを出力装置11cで所定の出力レベルまで増幅する。そして、基地通信部12が乱数列 R_i と鍵インデックス IK_i とを各移動端末局21a～21nに送信する（ステップ402）。

【0072】次に、移動端末局21から送信されてくる認証子を受信する（ステップ403）。なお、移動端末局21で得られる認証子については、移動端末局21の処理フローチャートで説明する。

【0073】さらに、秘密鍵データベース11aから秘密鍵 K_{si} を通信すべき移動端末局21に対応する秘密鍵 K_{si} を取り出す（ステップ404）。そして、この乱数列及び鍵インデックスに対して前処理として排他的論理和処理を行う（ステップ405）。

【0074】図17に前処理フローチャートを示す。図17において、前処理装置11jは取り出した秘密鍵 K_{si} と乱数列 R_i との排他的論理和を求める（ステップ

420)。そして、演算装置11dが乱数 R_i と秘密鍵 K_{si} との内積を演算して内積列 MS_i を求める(ステップ406)。

【0075】さらに、得られた内積列に基いて、後処理装置11eが転置処理やあるいは抽出処理を行うことにより認証子を求める(ステップ407)。次に、比較装置11gがステップ103で受信した移動端末局21の第2の認証子とステップ407で求められた第1の認証子との比較を行う(ステップ408)。

【0076】そして、移動端末局21が無線基地局10に正規に登録された端末局か否かを判別する(ステップ409)。すなわち、ステップ403で受信した移動端末局21の認証子と、ステップ407で求められた認証子とが一致するか否かを判別する。ここで、第1の認証子と第2の認証子とが一致する場合には、処理を終了する。そうでない場合には、ステップ401に戻る。

【0077】このような装置においては、前処理及び後処理が追加されているので、さらに秘密鍵の解読がしにくくなる。図18に移動端末局の処理フローチャートを示す。まず、各移動端末局21a~21nでは、無線基地局10から送信された鍵インデックス IK_i と乱数列 R_i の受信を待つ(ステップ411)。そして、入力装置31fが鍵インデックス IK_i と乱数列 R_i を受信すると、演算装置31dは鍵インデックス IK_i に対応する秘密鍵 K_i を取り出す(ステップ412)。

【0078】さらに、前処理装置31jが前処理として排他的論理和処理を行った後に(ステップ413)、演算装置31dは、ステップ411で受けた乱数列 R_i とステップ112で取り出した秘密鍵とから内積を演算して、内積列を求める(ステップ414)。

【0079】そして、後処理装置31eが後処理として内積列から抽出処理を行った後(ステップ415)、第2の認証子として無線基地局10に送信する(ステップ416)。

<実施例5>次に、本発明の実施例5について説明する。図19に実施例5の端末認証部45の構成ブロック図を示す。実施例5では、端末認証部45において、鍵インデックスを変換する変換装置11kを備える点が実施例4に対して異なる。図19において、変換装置11kは、鍵の変換方法を複数種類用意したものであり、複数種類の鍵インデックス IK_i により鍵データベース11aからの秘密鍵を変換処理、例えば転置処理、排他的論理和処理、換字処理を行う。

【0080】例えば、図21に示すように鍵インデックスが「00」である場合には転置前の鍵「 $K_1, K_2, K_3 \dots K_n$ 」を転置後の鍵「 $K_n, K_1, K_2 \dots K_{n-1}$ 」に転置する。

【0081】なお、換字処理とは、複数の換字テーブルを用意し、鍵インデックスの値に応じた換字テーブルを参照して鍵の換字を行うものである。この換字処理も転

置処理の一種である。

【0082】図20に実施例5の認証子発生部の構成ブロック図を示す。実施例5では、認証子発生部55において、鍵インデックスを変換する変換装置31kを備える点が実施例4に対して異なる。図20において、変換装置31kは、図19に示す変換装置11kと同一構成であり、複数種類の鍵インデックス IK_i により秘密鍵を変換処理、例えば図21に示すような転置処理を行う。

【0083】このような変換装置11k、31kを用いるので、認証子等の符号列が傍受されても、鍵インデックスによる鍵の転置処理によって、その内容を解析することはより困難となるので、通信内容の秘密性を確保することができる。

【0084】図22に実施例5の無線基地局の処理フローチャートを示す。このように構成された実施例5における無線基地局の処理を説明する。まず、無線基地局10において、乱数発生装置11bが乱数 R_i と鍵インデックス IK_i を発生し(ステップ501)、乱数列 R_i と鍵インデックス IK_i とを出力装置11cで所定の出力レベルまで増幅する。そして、基地通信部12が乱数列 R_i と鍵インデックス IK_i とを各移動端末局21a~21nに送信する(ステップ502)。

【0085】次に、移動端末局21から送信されてくる認証子を受信する(ステップ503)。秘密鍵データベース11aから秘密鍵 K_{si} を通信すべき移動端末局21に対応する秘密鍵を取り出す(ステップ504)。そして、変換装置11kが鍵インデックス IK_i により鍵の変換を行い(ステップ505)、前処理装置11jが変換された鍵と乱数列に対して前処理を行う(ステップ506)。

【0086】さらに、演算装置11dが乱数列 R_i と秘密鍵 K_{si} との内積を演算する(ステップ507)。得られた内積列に基いて、転置処理やあるいは抽出処理を行うことにより認証子を求める(ステップ508)。

【0087】そして、受信した移動端末局21の認証子とステップ508で求められた認証子との比較を行う(ステップ509)。移動端末局21が無線基地局10に正規に登録された端末局か否かを判別する(ステップ510)。すなわち、受信した移動端末局21の認証子と、ステップ508で求められた認証子とが一致するか否かを判別する。ここで、認証子同士が一致する場合には、処理を終了する。そうでない場合には、ステップ501に戻る。

【0088】図23に移動端末局の処理フローチャートを示す。まず、各移動端末局21a~21nでは、無線基地局10から送信された鍵インデックス IK_i と乱数列 R_i の受信を待つ(ステップ511)。そして、入力装置31fが鍵インデックス IK_i と乱数列 R_i を受信すると、演算装置31dは鍵インデックス IK_i に対応

する秘密鍵 K_i を取り出す(ステップ512)。

【0089】そして、変換装置31kが鍵インデックス IK_i により鍵の変換を行い(ステップ513)、前処理装置31jが変換された鍵と乱数列に対して前処理を行う(ステップ514)。さらに、演算装置31dは、ステップ511で受けた乱数列 R_i と秘密鍵とから内積を演算して、内積列を求め(ステップ515)、後処理を行って(ステップ516)、認証子を送信する(ステップ517)。

<実施例6>次に、本発明の実施例6について説明する。図24に実施例6の端末認証部の構成ブロック図を示す。実施例6では、端末認証部46において、前処理及び後処理に対して選択すべき複数種類の交換方法を用意したものであり、鍵インデックス IK_i の値と複数種類の交換内容とを対応付けた変換データベース11mを備える。図24において、変換データベース11mは、図25に示すような鍵インデックスと交換内容(論理和、論理積、排他的論理和、転置、換字等)とを対応付けて格納している。

【0090】例えば、鍵インデックスが「000」である場合には前処理装置11j及び後処理装置11eで行うべき処理として、「論理和」が変換データベース11mから選択される。

【0091】図26に実施例6の認証子発生部の構成ブロック図を示す。実施例6では、認証子発生部56において、図24に示した変換データベース11mと同一構成の変換データベース31mを備える。

【0092】このような変換データベース11m、31mを用いるので、各種の変換処理を適宜選択でき、通信内容の秘密性を確保することができる。図27に実施例6の無線基地局の処理フローチャートを示す。このように構成された実施例6における無線基地局の処理を説明する。まず、無線基地局10において、乱数発生装置11bが乱数 R_i と鍵インデックス IK_i を発生し(ステップ601)、乱数列 R_i と鍵インデックス IK_i とを出力装置11cで所定の出力レベルまで増幅する。

【0093】そして、基地通信部12が乱数列 R_i と鍵インデックス IK_i とを各移動端末局21a~21nに送信する(ステップ602)。次に、移動端末局21から送信されてくる認証子を受信する(ステップ603)。秘密鍵データベース11aから通信すべき移動端末局21に対応する秘密鍵を取り出す(ステップ604)。鍵インデックスにより図25に示すいずれかの交換、例えば論理和を選択し(ステップ605)、鍵に対して前処理として論理和処理を行う(ステップ606)。

【0094】さらに、乱数列 R_i と秘密鍵 K_{si} との内積を演算する(ステップ607)。得られた内積列に基づいて、転置処理やあるいは抽出処理を行うことにより認証子を求める(ステップ608)。

【0095】受信した移動端末局21の認証子とステップ608で求められた認証子との比較を行う(ステップ609)。移動端末局21が無線基地局10に正規に登録された端末局か否かを判別する(ステップ610)。すなわち、受信した移動端末局21の認証子と、求められた認証子とが一致するか否かを判別する。ここで、認証子同士が一致する場合には、処理を終了する。そうでない場合には、ステップ601に戻る。

【0096】図28に移動端末局の処理フローチャートを示す。まず、各移動端末局21a~21nでは、無線基地局10から送信された鍵インデックス IK_i と乱数列 R_i の受信を待つ(ステップ611)。そして、入力装置31fが鍵インデックス IK_i と乱数列 R_i を受信すると、演算装置31dは鍵インデックス IK_i に対応する秘密鍵 K_i を取り出す(ステップ612)。

【0097】そして、鍵インデックスにより図25に示すいずれかの交換、例えば論理和を選択し(ステップ613)、鍵に対して前処理として論理和処理を行う(ステップ614)。演算装置31dは、乱数列 R_i と秘密鍵とから内積を演算して、内積列を求める(ステップ615)。

【0098】次に、得られた内積列に基づいて、転置処理やあるいは抽出処理を行うことにより認証子を求め(ステップ616)、認証子を無線基地局10に送信する(ステップ617)。

【0099】以上実施例1から実施例6まで説明したが、これらの実施例によれば、移動端末局毎に複数種類の秘密鍵を有するとともに複数種類の秘密鍵のいずれかを鍵インデックスにより指定できるので、移動端末局毎に秘密鍵が1つの秘密鍵よりも複数種類増加するため、傍受者には秘密鍵の解読がより困難になる。

【0100】すなわち、線形独立な乱数式 R_i が n 個とそれに対応する内積列 MS_i が傍受者にわかるならば、利用者の秘密鍵は解読できる。従って、実施例によれば、1つの秘密鍵を用いるよりも約 m 倍(K_{si} の s を1から m とした場合)の乱数と認証子とのペアが必要となるため、より安全な端末認証を行うことができる。

【0101】また、前処理、後処理、交換処理などの処理を加えることにより、さらに、秘密鍵の安全性を確保できる。なお、本発明は実施例1ないし実施例6に限定されるものではない。前記実施例では、無線基地局10で移動端末局21の認証を行うようにしたが、移動端末局21に前記実施例で説明した乱数発生装置を備えるようにしてよい。

【0102】この場合には、移動端末局10が乱数列及び認証子を無線基地局10に送信する。このような構成であっても、移動端末局を認証することができる。

【0103】

【発明の効果】本発明によれば、移動端末局毎に複数種類の秘密鍵を有するとともに複数種類の秘密鍵のいずれ

かを鍵インデックスにより指定できるので、移動端末局毎に秘密鍵が1つの秘密鍵よりも複数種類増加するため、傍受者には秘密鍵の解読がより困難になる。従って、よりデータの秘密性を保持することができる。

【図面の簡単な説明】

【図1】本発明の原理図である。

【図2】本発明の実施例1の構成ブロック図である。

【図3】実施例1の端末認証部の構成ブロック図である。

【図4】鍵インデックスと秘密鍵との対応を示す図である。

【図5】認証子の決定方法の一例を示す図である。

【図6】実施例1の認証子発生部の構成ブロック図である。

【図7】実施例1の無線基地局処理フローチャートである。

【図8】実施例1の端末処理フローチャートである。

【図9】実施例1の内積処理フローチャートである。

【図10】実施例1の後処理フローチャートである。

【図11】実施例2の後処理フローチャートである。

【図12】転置処理の一例を示す図である。

【図13】実施例3の後処理フローチャートである。

【図14】実施例4の端末認証部の構成ブロック図である。

【図15】実施例4の認証子発生部の構成ブロック図である。

【図16】実施例4の無線基地局の処理フローチャートである。

【図17】実施例4の前処理フローチャートである。

【図18】実施例4の端末処理フローチャートである。

【図19】実施例5の端末認証部の構成ブロック図である。

【図20】実施例5の認証子発生部の構成ブロック図である。

【図21】変換処理の一例を示す図である。

*

*【図22】実施例5の無線基地局の処理フローチャートである。

【図23】実施例5の端末処理フローチャートである。

【図24】実施例6の端末認証部の構成ブロック図である。

【図25】変換処理の他の一例を示す図である。

【図26】実施例6の認証子発生部の構成ブロック図である。

【図27】実施例6の無線基地局の処理フローチャートである。

【図28】実施例6の端末処理フローチャートである。

【符号の説明】

10・・・無線基地局

11・・・端末認証部

12・・・基地通信部

13, 24a~24n・・・制御部

21a~21n・・・移動端末局

22a~22n・・・認証子発生部

23a~23n・・・移動通信部

11a・・・鍵データベース

11b・・・乱数発生装置

11c, 31c・・・出力装置

11d, 31d・・・演算装置

11e, 31e・・・後処理装置

11f, 31f・・・入力装置

11g・・・比較装置

11h, 31h・・・制御回路

11k・・・変換装置

11m・・・変換データベース

IKi・・・鍵インデックス

Ksi・・・秘密鍵

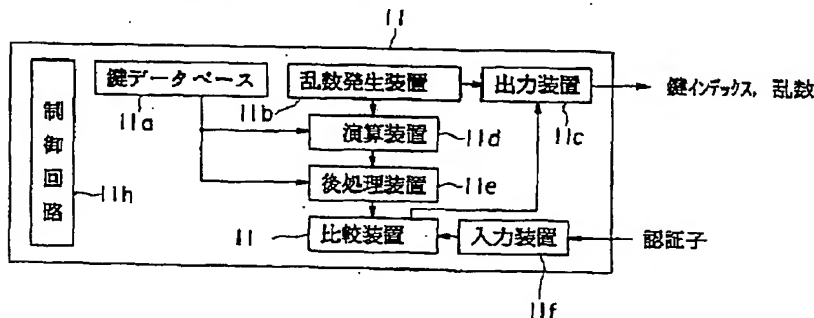
Si・・・認証子

MSi・・・内積列

Ri・・・乱数列

【図3】

実施例1の端末認証部の構成ブロック図

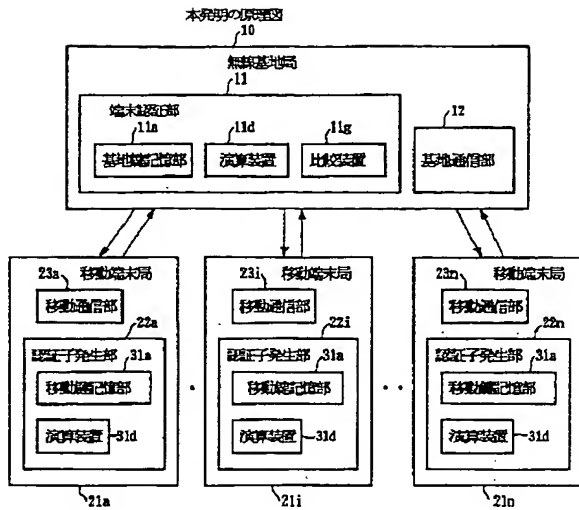


【図4】

鍵インデックスと秘密鍵との対応を示す図

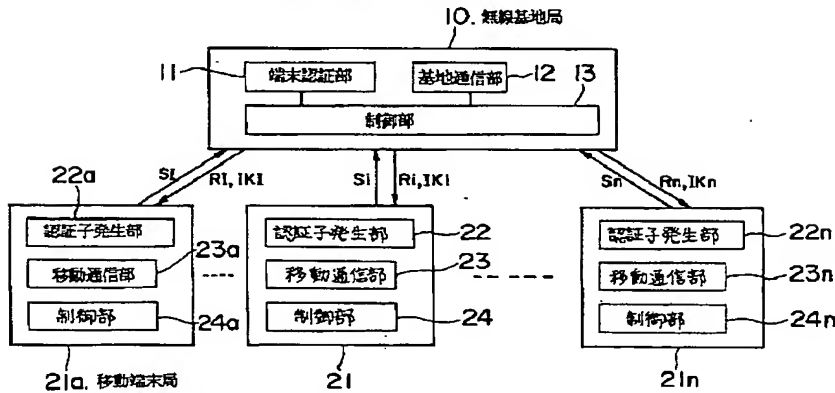
鍵インデックスIKi	秘密鍵Ksi
IK1i	K1i
IK2i	K2i
IK3i	K3i
IK4i	K4i
⋮	⋮
IKmi	Kmi

【図1】



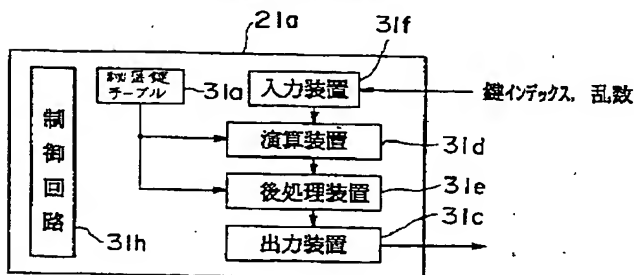
【図2】

本発明の実施例1の構成ブロック図



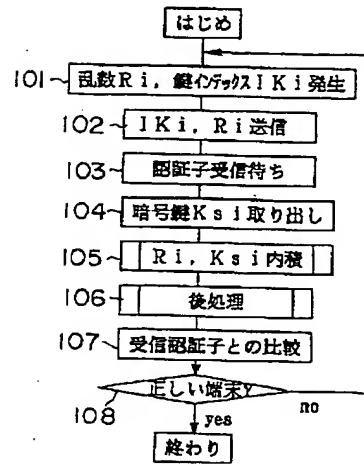
【図6】

実施例1の認証子発生部の構成ブロック図



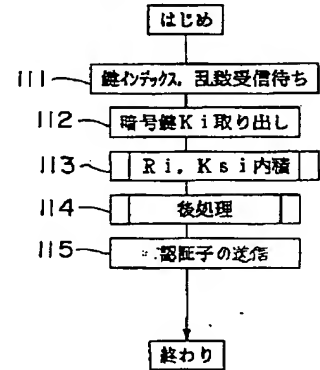
【図7】

実施例1の無線基地局処理フローチャート



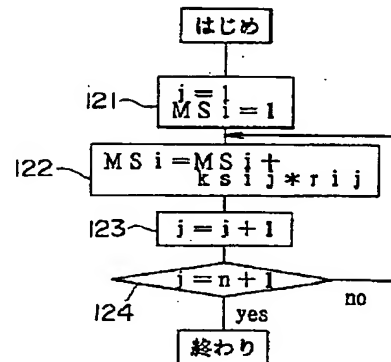
【図8】

実施例1の端末処理フローチャート



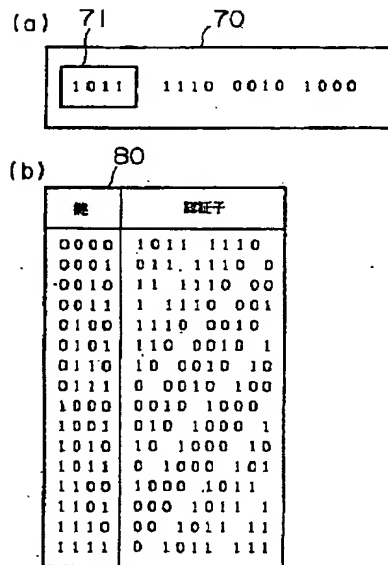
【図9】

実施例1の内積処理フローチャート



【図5】

証憑子の決定方法の一例を示す図



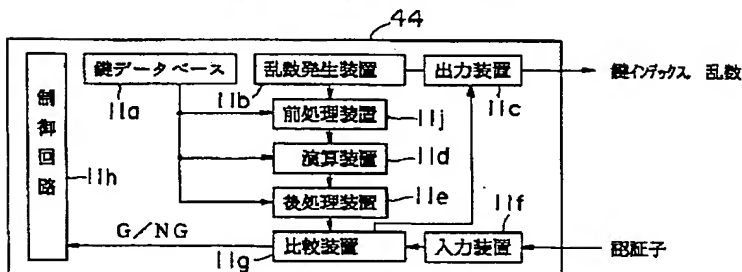
【図12】

転置処理の一例を示す図

鍵	転置前データ	転置後データ
000	A ₁ A ₂ A ₃ ----A _n	A _n A ₁ A ₂ ----A _{n-1}
010	A ₃ A ₁ A ₂ ----A _n	A ₁ A ₃ A ₂ ----A _n
⋮	⋮	⋮

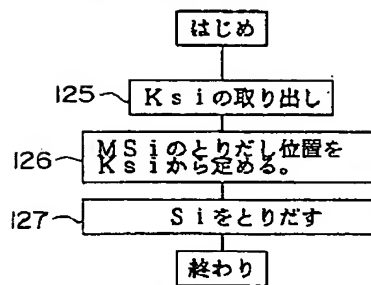
【図14】

実施例4の端末認証部の構成ブロック図



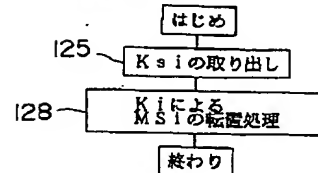
【図10】

実施例1の後処理フローチャート



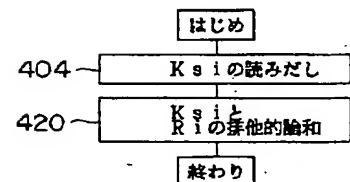
【図11】

実施例2の後処理フローチャート



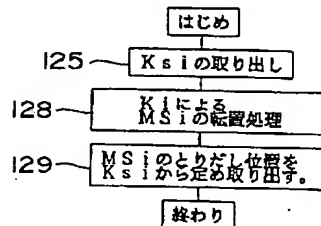
【図17】

実施例4の前処理フローチャート



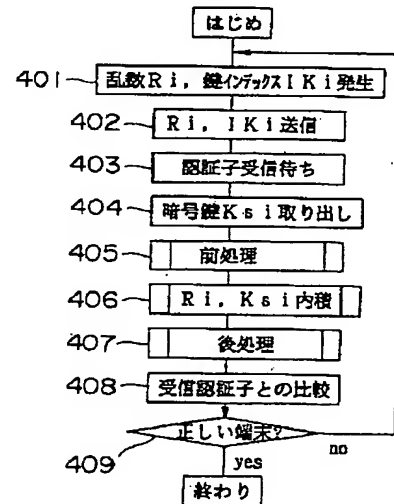
【図13】

実施例3の後処理フローチャート



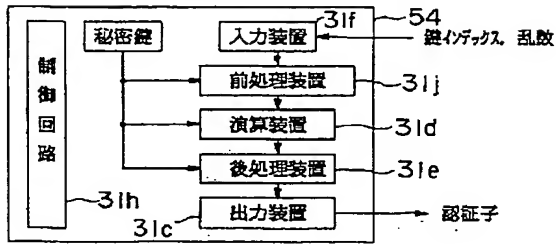
【図16】

実施例4の無線基地局の処理フローチャート



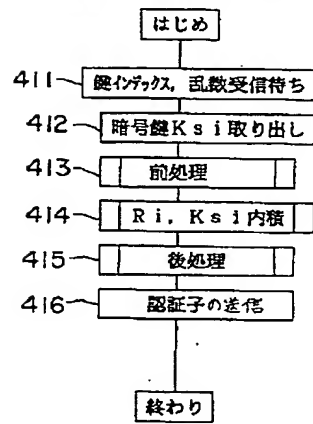
【図 15】

実施例 4 の認証子発生部の構成ブロック図



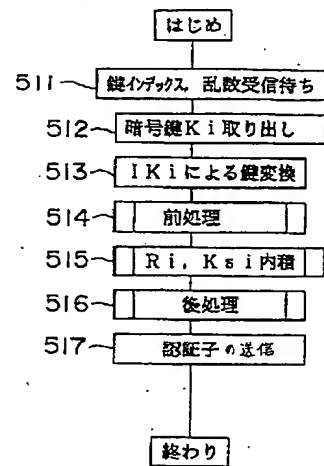
【図 18】

実施例 4 の端末処理フローチャート



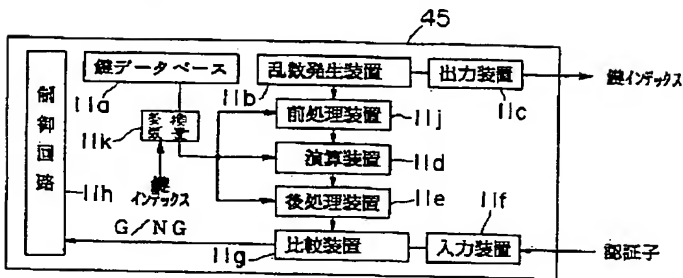
【図 23】

実施例 5 の端末処理フローチャート



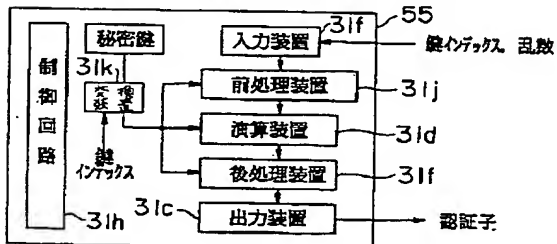
【図 19】

実施例 5 の端末認証部の構成ブロック図



【図 20】

実施例 5 の認証子発生部の構成ブロック図



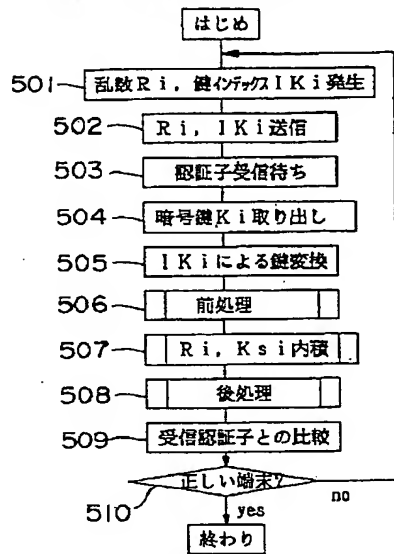
【図 21】

変換処理の一例を示す図

鍵インデックス	転置前の鍵	転置後の鍵
00	$K_1 K_2 K_3 \dots K_n$	$K_n K_1 K_2 \dots K_{n-1}$
01	$K_2 K_3 K_1 \dots K_n$	$K_3 K_1 K_2 \dots K_n$
⋮	⋮	⋮

【図22】

実施例5の無線基地局の処理フローチャート



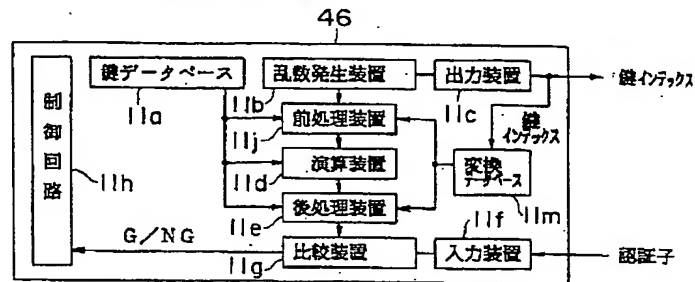
【図25】

変換処理の他の一例を示す図

鍵インデックス	変換内容
000	論理和
001	論理積
010	排他的論理和
011	転置
100	複写
...	...

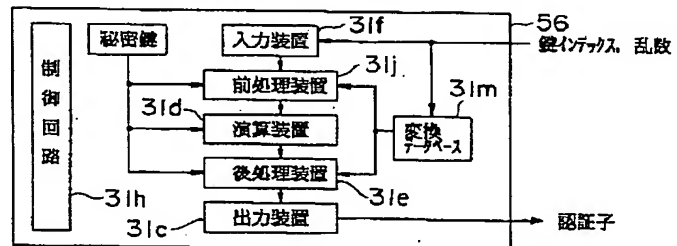
【図24】

実施例6の端末認証部の構成ブロック図



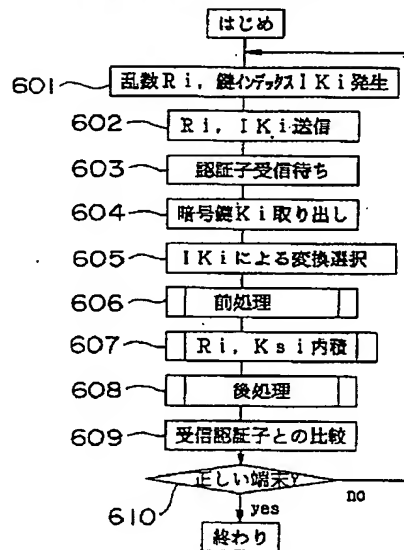
【図26】

実施例6の認証子発生部の構成ブロック図



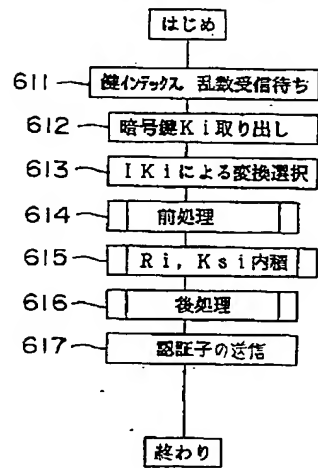
【図27】

実施例6の無線基地局の処理フローチャート



【図 28】

実施例 6 の端末処理フローチャート



フロントページの続き

(51)Int.Cl.⁶

G 0 9 C 1/00

H 0 4 Q 7/38

識別記号

3 1 0

庁内整理番号

9364-5L

F I

技術表示箇所

[Embodiments]

Embodiments of the communication terminal authentication device of the present invention will now be described. Fig. 2 is a block diagram of a first embodiment of the communication terminal authentication device of the present invention.

(First Embodiment)

As shown in Fig. 2, the communication terminal authentication device is constituted by a wireless base station 10 and a plurality of mobile terminal stations 21, wherein wireless communication is performed between the wireless base station 10 and each mobile terminal station 21 (21a to 21n).

[0027]

The wireless base station 10 comprises a terminal authentication portion 11, a base communication portion 12, and a control portion 13. Each mobile terminal station 21 (21a to 21n) comprises an authenticator generating portion 22 (22a to

22n), a mobile communication portion 23 (23a to 23n), and a control portion 24 (24a to 24n).

[0028]

In the wireless base station 10, the terminal authentication portion 11 stores in a key database 11a a plurality of types of secret keys K_{si} (K_{s11} , K_{s12} ..., K_{sin} , where s is m equal to or greater than 1) and corresponding key indices IK_i ($s = IK_i$, IK_i is m equal to or greater than 1) for each mobile terminal station 21 (21a to 21n) with which a communication connection is possible. The terminal authentication portion 11 also generates random number sequences R_i ($ri1$, $ri2$..., rin) (each element having a predetermined bit width) and outputs these sequences to the mobile terminal stations 21 (21a to 21n).

[0029]

The wireless base station 10 compares a first authenticator $MS1i$ obtained by calculating the inner product of the secret keys K_{si} (K_{s11} , K_{s12} ..., K_{sin}) specified by the key

indices IK_i and the outputted random number sequences R_i (ri_1 , ri_2 ..., ri_n) with a second authenticator received from the mobile terminal station 21, and outputs a communication enabling signal or a communication denial signal.

[0030]

The base communication portion 12 transmits the random number sequence R_i and key index IK_i and receives the second authenticator $MS2_i$. The control portion 13 controls the entire wireless base station 10 and also controls operations of the terminal authentication portion 11 and base communication portion 12.

[0031]

Note that the random number sequence R_i and secret key are each 512 bit code sequences with an element length of 8 bits. In the mobile terminal stations 21a to 21n, the mobile communication portions 23a to 23n receive the random number sequence R_i and key index IK_i respectively, and transmit the

second authenticator $MS2i$. The authenticator generating portions 22a to 22n output the second authenticator $MS2i$, which is obtained by calculating the inner product of the secret key K_{si} from among the plurality of types of secret keys K_{si} which corresponds to the key index IK_i and the received random number sequence R_i , to the wireless base station 10.

[0032]

The control portions 24a to 24n control the entirety of the mobile terminal stations 21a to 21n and perform movement control of the mobile communication portions 23a to 23n and authenticator generating portions 22a to 22n.

[0033]

Next, the specific constitution of the terminal authentication portion 11 provided in the wireless base station 10 and the authenticator generating portion 23 provided in the mobile terminal station 21 will be described. Fig. 3 is a block diagram of the terminal authentication portion 11 of the first

embodiment. The terminal authentication portion 11 comprises the key database 11a, a random number generating device 11b, an output device 11c, a calculating device 11d, a post-processing device 11e, an input device 11f, a comparing device 11g, and a control circuit 11h for controlling each of these devices.

[0034]

The key database 11a stores the plurality of types of secret keys K_{si} ($K_{s1}, K_{s2}, \dots, K_{sn}$) and corresponding key indices IK_i ($s = IK_i$, IK_i is m equal to or greater than 1) for each mobile terminal station 21a to 21i to 21n with which a communication connection is possible. Here, i indicates an arbitrary mobile terminal number, and is n equal to or greater than 1. n indicates the total number of terminals. s is m equal to or greater than 1, and thus m types of secret keys K_{si} are prepared for each mobile terminal station.

[0035]

If this is expressed as a mathematical expression, the following expression (1) is obtained.

$$s = IK_i \quad (1)$$

Fig. 4 shows the relationship between the plurality of types of secret keys and key indices stored in the key database. As shown in Fig. 4, a plurality of types of key indices IK_i (IK_{1i} , IK_{2i} ..., IK_{mi}) corresponds to a plurality of types of secret keys K_{si} (K_{1i} , K_{2i} ..., K_{mi}) in respect of the mobile terminal station 21i.

[0036]

The control portion 13 extracts from the key database 11a the secret key K_{si} which corresponds to the key index IK_i . In accordance with an instruction from the control portion 13 shown in Fig. 2, the random number generating device 11b generates the random number sequence R_i which changes according to the key index IK_i and the date and time, for example.

[0037]

The output device 11c amplifies the random number sequence R_i generated by the random number generating device 11b, the key index IK_i , and a predetermined enabling signal YN which is outputted from the comparing device 11g to be described below to a constant output level and outputs same.

[0038]

The calculating device 11d calculates the respective inner products of the secret keys K_{si} stored in the key database 11a and the random number sequences R_i generated by the random number generating device 11b to determine an inner product sequence MS_{1i} .

[0039]

If this is expressed using a mathematical expression, the following expression (2) is obtained.

$$MS_i = \sum K_{sij} \times r_{ij} \quad (2)$$

Note that j is caused to change from 1 to n .

[0040]

The post-processing device 11e performs post-processing based on the secret key K_{si} on the inner product sequence MS_{li} obtained by the calculating device 11d and thereby determines the first authenticator S_{li} . If this is expressed using a mathematical expression, the following expression (3) is obtained.

[0041]

$$S_i = TK_i (MS_i) \quad (3)$$

Here, $TK_i (MS_i)$ is a function for extracting from MS_i data serving as S_i regarding a position determined by the key. In other words, the bit length of S_i is set as N_s , and the bit length of MS_i is set as N_m . At this time, N_m is greater than N_s , and the extraction position of S_i varies in accordance with the value of K_i .

[0042]

For example, Fig. 5 shows an embodiment of an authenticator determining method. Fig. 5(a) shows an

embodiment of the inner product sequence MS_i , and Fig. 5(b) shows a table 80 of corresponding keys K_i and authenticators Si . Here, for ease, the inner product sequence MS_i has been set at 16 bits and the authenticators Si at 8 bits. In Fig. 5(a), an inner product sequence 70 is set at 16 bits and a key 71 is the leading 4 bits.

[0043]

In the table 80 shown in Fig. 5(b), when the key is "0000", the eight bits "10111110" from the first (most significant) bit are the authenticator Si . When the key is "0001", the eight bits "01111100" from the second bit are the authenticator Si .

[0044]

Note that in contrast to the determining method for the authenticator Si described above, selections may be made successively from the least significant bit of the inner product sequence. The input device 11f receives the second authenticator $S2_i$ received by the base communication portion

12. The comparing device 11g compares the authenticator S1i outputted from the post-processing device 11e to the authenticator S2i outputted from the input device 11f and outputs a predetermined enabling signal YN. More specifically, a communication enabling signal is outputted if the authenticator S1i and the authenticator S2i outputted from the input device 11f match, and if not, a communication denial signal is outputted.

FIG. 1

A: PRINCIPLE DIAGRAM OF PRESENT INVENTION

10 WIRELESS BASE STATION

11 TERMINAL AUTHENTICATION PORTION

11a BASE KEY STORAGE PORTION

11d CALCULATING DEVICE

11g COMPARING DEVICE

12 BASE COMMUNICATION PORTION

21a, 21i, 21n MOBILE TERMINAL STATION

23a, 23i, 23n MOBILE COMMUNICATION PORTION

22a, 22i, 22n AUTHENTICATOR GENERATING PORTION

31a, 31a, 31a MOBILE KEY STORAGE PORTION

31d, 31d, 31d CALCULATING DEVICE

FIG. 2

A: BLOCK DIAGRAM OF FIRST EMBODIMENT OF PRESENT INVENTION

10 WIRELESS BASE STATION

11 TERMINAL AUTHENTICATION PORTION

12 BASE COMMUNICATION PORTION

13 CONTROL PORTION

21a, 21, 21n MOBILE TERMINAL STATION

22a, 22, 22n AUTHENTICATOR GENERATING PORTION

23a, 23, 23n MOBILE COMMUNICATION PORTION

24a, 24, 24n CONTROL PORTION

FIG. 3

A: BLOCK DIAGRAM OF TERMINAL AUTHENTICATION PORTION OF FIRST
EMBODIMENT

11h CONTROL CIRCUIT

11a KEY DATABASE

11b RANDOM NUMBER GENERATING DEVICE

11d CALCULATING DEVICE

11e POST-PROCESSING DEVICE

11[g] COMPARING DEVICE

11c OUTPUT DEVICE

11f INPUT DEVICE

B: KEY INDICES, RANDOM NUMBERS

C: AUTHENTICATOR

FIG. 4

A: VIEW SHOWING RELATIONSHIP BETWEEN KEY INDICES AND SECRET KEYS

B: KEY INDEX IK_i

C: SECRET KEY K_{si}

FIG. 5

A: VIEW SHOWING ONE EMBODIMENT OF AUTHENTICATOR DETERMINING METHOD

B: KEY

C: AUTHENTICATOR

FIG. 6

A: BLOCK DIAGRAM OF AUTHENTICATOR GENERATING PORTION OF FIRST
EMBODIMENT

31h CONTROL CIRCUIT

31a SECRET KEY TABLE

31f INPUT DEVICE

31d CALCULATING DEVICE

鍵インデックスと秘密鍵との対応を示す図

インデックス IK_i	秘密鍵 K_{si}
$IK1$	$K1$
$IK2$	$K2$
$IK3$	$K3$
$IK4$	$K4$
\vdots	\vdots
IK_m	K_m

31e POST-PROCESSING DEVICE

31c OUTPUT DEVICE

B: KEY INDICES, RANDOM NUMBERS

FIG. 1

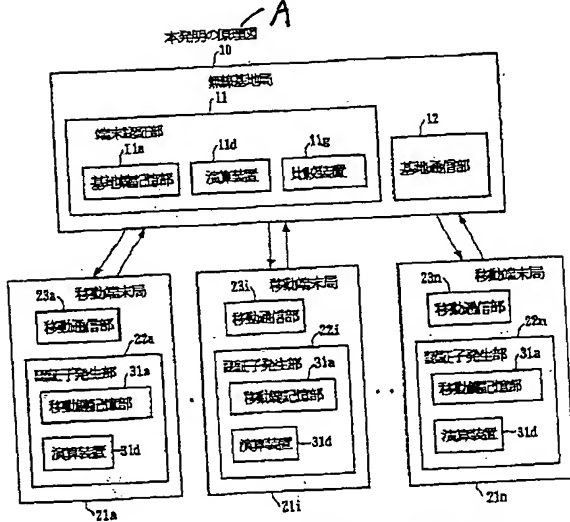


FIG. 2

本発明の実施例 1 の構成ブロック図

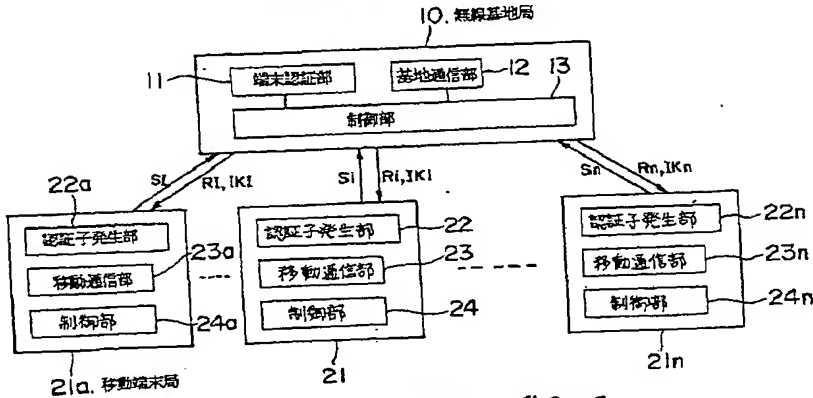


FIG. 3

実施例 1 の端末認証部の構成ブロック図

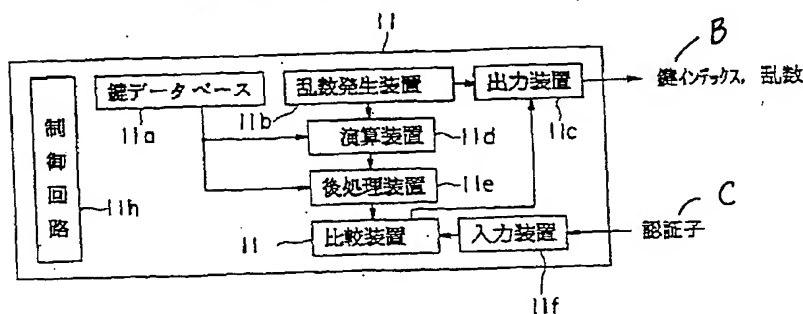


FIG. 5

鍵証子の決定方法の一例を示す図

(a)

71	70
1011	1110 0010 1000

(b)

鍵	鍵証子
0000	1011 1110
0001	011 1110 0
0010	11 1110 00
0011	1 1110 001
0100	1110 0010
0101	110 0010 1
0110	10 0010 10
0111	0 0010 100
1000	0010 1000
1001	010 1000 1
1010	10 1000 10
1011	0 1000 101
1100	1000 1011
1101	000 1011 1
1110	00 1011 11
1111	0 1011 111

FIG. 6

実施例 1 の鍵証子発生部の構成ブロック図

